UNIVERSITY OF THESSALY
SCHOOL OF ENGINEERING
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

Design and implementation of Reliability aware Hardware Trojans and attacks

A dissertation submitted in partial fulfillment of the requirements

for the degree of Doctor of Philosophy

Alexandra Takou

2025

UNIVERSITY OF THESSALY
SCHOOL OF ENGINEERING
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

Design and implementation of Reliability aware Hardware Trojans and attacks

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy

Alexandra Takou

2025

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Σχεδιασμός και υλοποίηση Hardware Trojans και επιθέσεων που λαμβάνουν υπόψιν το Reliability

Διατριβή η οποία υποβλήθηκε για τη μερική εκπλήρωση
των υποχρεώσεων απόκτησης του Διδακτορικού Διπλώματος

Αλεξάνδρα Τάκου

2025

UNIVERSITY OF THESSALY
SCHOOL OF ENGINEERING
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

Design and implementation of Reliability aware Hardware Trojans and attacks

PhD Dissertation

Alexandra Takou

Advisory committee

George Stamoulis, Professor, Univ. of Thessaly (Supervisor)

Nestor Evmorfopoulos, Professor, Univ. of Thessaly

Antonis Dadaliaris, Assistant Professor, Univ. of Thessaly

Examination committee

George Stamoulis, Professor, Univ. of Thessaly (Supervisor)

Nestor Evmorfopoulos, Professor, Univ. of Thessaly

Antonis Dadaliaris, Assistant Professor, Univ. of Thessaly

Michael Dossis, Professor, University of Western Macedonia

Georgios Panagopoulos, Assistant Professor, National Technical University of Athens

Dimitris Karampatzakis, Assistant Professor, Democritus University of Thrace

Alexandros Chroneos, Professor, University of Thessaly

2025

DISCLAIMER ON ACADEMIC ETHICS AND INTELLECTUAL PROPERTY RIGHTS

Being fully aware of the implications of copyright laws, I expressly state that this PH.D. dissertation, as well as the electronic files and source codes developed or modified in the course of this thesis, are solely the product of my personal work and do not infringe any rights of intellectual property, personality and personal data of third parties, do not contain work / contributions of third parties for which the permission of the authors / beneficiaries is required and are not a product of partial or complete plagiarism, while the sources used are limited to the bibliographic references only and meet the rules of scientific citing. The points where I have used ideas, text, files and / or sources of other authors are clearly mentioned in the text with the appropriate citation and the relevant complete reference is included in the bibliographic references section. I also declare that the results of the work have not been used to obtain another degree. I fully, individually and personally undertake all legal and administrative consequences that may arise in the event that it is proven, in the course of time, that this thesis or part of it does not belong to me because it is a product of plagiarism.

The declarant

Alexandra Takou

Acknowledgements

As this journey reaches its end, I would like to express my deepest gratitude first and foremost to my supervisor, Prof. George Stamoulis, for his unwavering belief, support, and encouragement throughout my PhD journey. Their insightful advice, expertise, and patience were invaluable, and I feel incredibly fortunate to have had the opportunity to work with such an inspiring mentor.

I would also like to extend my thanks to the members of my dissertation committee, Prof. Nestor Evmorfopoulos and Assistant Prof. Antonios Dadaliaris, for their constructive feedback and suggestions, which significantly improved the quality of this research.

A special thanks to the members of the ERL lab of the University of Thessaly for their collaboration, and assistance in my research, for being wonderful colleagues throughout my studies, and for teaching me valuable lessons that I will carry with me for the rest of my life. Your contributions were essential to the success of this work and my journey after this.

I am grateful to my colleagues and friends at the University of Thessaly for creating a supportive and intellectually stimulating environment. The stimulating discussions and shared experiences with you all made this journey enjoyable and rewarding.

To my family, your love and belief in me have been my anchor. Thank you, mom, dad, and Dr sister, for always being there, offering encouragement, and providing a source of strength, especially during the challenging moments. Your sacrifices and unwavering support have made all the difference.

Lastly, I want to thank all the individuals who have been part of my academic and personal growth over the years. Whether through direct collaboration, encouragement, or simply being part of my journey, your influence has made this achievement possible.

PhD Dissertation

Design and implementation of Reliability aware Hardware Trojans and attacks

Alexandra Takou

Abstract

Hardware security has been a great concern in the field of Integrated Circuits (IC) design in the last decades. Specifically, hardware trojans pose the greatest threat to the security of ICs. A hardware trojan is logic inserted in any design, exploiting the design's characteristics with a malicious intent. Leaking information, changing the expected behavior of the circuit, or simply terminating its function altogether are some of the most serious implications of a trojan. A category of especially detrimental hardware attacks aims at exploiting the reliability of the IC, called reliability hardware trojans. Phenomena such as Electromigration (EM) and Single Event Transient (SET) pulses can be exaggerated using a trojan to prevent the intended behavior. The former can render a path inactive earlier than the specifications, the latter can generate a soft error, which, although is a temporary error, can still disturb the functionality of the circuit. Therefore, they need to be thoroughly studied and explored. To further aid the development of satisfactory countermeasures and detection techniques, challenging and realistic benchmarks need to be generated to evaluate the aforementioned techniques.

In this dissertation, three examples of hardware attacks on reliability phenomena are described. Each attack's respective hardware trojan is designed and implemented, accompanied by an algorithm to discover the optimal points of attack. The first two examples focus on exploiting the EM phenomenon, while the third focuses on the radiation-induced SET pulses and the generation of soft errors. Firstly, an attack on power grid structures to aggravate the EM phenomenon is described. The attack is achieved by removing the crucial decoupling capacitances, shortening the lifetime of the power grid. The second implements an attack on clock tree networks that accelerates the aging of a branch by adding a resistive element at the point of attack. The power grid and the clock tree are two of the main components of a chip, so an unexpected failure of them will render the whole IC non-functional. Last,

a theoretical approach to implementing and injecting into a design a SET-based hardware trojan is presented. The trojan widens the glitch enough to maximize the chances a soft error will occur at the memory cell on the path it is inserted. For the first methodology, several large-scale power grid benchmarks from the OpenROAD project are used to evaluate the efficiency and validity of the method, while for the evaluation of the second, three clock tree networks with different sizes were extracted from a set of microprocessor designs with random control logic and datapath. Since this trojan is only described and not yet implemented, an increase of 15% in the SET glitch's width was applied and several of the ISCAS '98 benchmarks were used to evaluate the effectiveness of the placing technique.

Keywords

Hardware Security; Hardware Trojan; Reliability, Electromigration; Single Event Transient; Soft errors; Power Grid network; Clock Tree network; SET-triggered; Pulse broadening; Benchmarks.

Διδακτορική Διατριβή

Σχεδιασμός και υλοποίηση Hardware Trojans και επιθέσεων που λαμβάνουν υπόψιν το Reliability

Αλεξάνδρα Τάκου

Περίληψη

Η ασφάλεια υλικού αποτελεί μεγάλο μέλημα στον τομέα της σχεδίασης ολοκληρωμένων κυκλωμάτων (ΟΚ) τις τελευταίες δεκαετίες. Συγκεκριμένα, τα hardware trojans αποτελούν τη μεγαλύτερη απειλή για την ασφάλεια των ολοκληρωμένων κυκλωμάτων. Το hardware trojan είναι λογική που εισάγεται σε οποιοδήποτε σχέδιο κυκλώματος, εκμεταλλευόμενη τα χαρακτηριστικά του με κακόβουλη πρόθεση. Η διαρροή πληροφοριών, η αλλαγή της αναμενόμενης συμπεριφοράς του κυκλώματος ή απλά ο ολοκληρωτικός τερματισμός της λειτουργίας του είναι μερικές από τις πιο σοβαρές επιπτώσεις ενός trojan. Μια κατηγορία ιδιαίτερα επιζήμιων επιθέσεων υλικού εκμεταλλεύεται την αξιοπιστία του ολοκληρωμένου κυκλώματος, οι οποίες ονομάζονται hardware trojans αξιοπιστίας (reliability hardware trojans). Φαινόμενα όπως η ηλεκτρομετανάστευση (Electromigration - EM) και οι παλμοί Single Event Transient (SET) μπορούν να υπερτονιστούν με τη χρήση ενός trojan για να αποτρέψουν την προβλεπόμενη συμπεριφορά. Το πρώτο μπορεί να καταστήσει ενα μονοπάτι του ΟΚ ανενεργό νωρίτερα από τις προδιαγραφές, το δεύτερο μπορεί να δημιουργήσει ένα Μεταβατικό Σφάλμα, το οποίο, αν και είναι προσωρινό σφάλμα, μπορεί να διαταράξει τη λειτουργικότητα του κυκλώματος. Ως εκ τούτου, πρέπει να μελετηθούν και να διερευνηθούν διεξοδικά. Για να βοηθηθεί περαιτέρω η ανάπτυξη ικανοποιητικών αντιμέτρων και τεχνικών ανίχνευσης, πρέπει να δημιουργηθούν απαιτητικά και ρεαλιστικά benchmarks για την αξιολόγηση των προαναφερθέντων τεχνικών.

Στην παρούσα διατριβή περιγράφονται τρία παραδείγματα επιθέσεων υλικού σε φαινόμενα αξιοπιστίας. Σχεδιάζεται και υλοποιείται το hardware trojan για κάθε επίθεση, συνοδευόμενος από έναν αλγόριθμο για την ανακάλυψη των βέλτιστων σημείων επίθεσης. Τα δύο πρώτα παραδείγματα επικεντρώνονται στην εκμετάλλευση του φαινομένου της ηλεκτρομετανάστευσης, ενώ το τρίτο εστιάζει στους παλμούς SET που προκαλούνται από ακτινοβολία και

στη δημιουργία μεταβατικών σφαλμάτων. Πρώτον, περιγράφεται μια επίθεση στις δομές του ηλεκτρικού δικτύου για την επιδείνωση του φαινομένου ηλεκτρομετανάστευσης. Η επίθεση επιτυγχάνεται με την αφαίρεση των κρίσιμων χωρητικοτήτων αποσύζευξης, μειώνοντας τη διάρκεια ζωής του δικτύου τροφοδοσίας. Η δεύτερη υλοποιεί μια επίθεση σε δίκτυα δέντρων ρολογιού που επιταχύνει τη γήρανση ενός κλάδου με την προσθήκη ενός ωμικού στοιχείου στο σημείο της επίθεσης. Το δίκτυο ισχύος και το δέντρο ρολογιού είναι δύο από τα κύρια στοιχεία ενός κυκλώματος, οπότε μια απροσδόκητη αποτυχία τους θα καταστήσει ολόκληρο το ΟΚ μη λειτουργικό. Τέλος, παρουσιάζεται μια θεωρητική προσέγγιση για την υλοποίηση και την εισαγωγή σε ένα κύκλωμα ενός hardware trojan με βάση την ευαισθησία της πύλης σε SET. Το hardware trojan διευρύνει τη δυσλειτουργία αρκετά ώστε να μεγιστοποιήσει τις πιθανότητες να συμβεί ένα μεταβατικό σφάλμα στο στοιχείο μνήμης στη διαδρομή που εισάγεται. Για την αξιολόγηση της αποτελεσματικότητας και της εγκυρότητας της πρώτης μεθοδολογίας χρησιμοποιούνται διάφορα μεγάλης κλίμακας benchmarks δικτύων ισχύος από το πρόγραμμα OpenROAD, ενώ τη δεύτερη μεθοδολογίας εξήχθησαν τρία δίκτυα δέντρων ρολογιού με διαφορετικά μεγέθη από ένα σύνολο κυκλωμάτων μικροεπεξεργαστών με τυχαία λογική ελέγχου και μονοπάτι δεδομένων. Δεδομένου ότι το τελευταίο trojan περιγράφεται θεωρητικά μόνο, εφαρμόστηκε αύξηση κατά 15% στο πλάτος της δυσλειτουργίας SET και χρησιμοποιήθηκαν διάφορα από τα benchmarks του ISCAS ’98 για να αξιολογηθεί η τεχνική τοποθέτησης ως προς την αποτελεσματικότητά της.

Λέξεις Κλειδιά

Ασφάλεια Υλικού; Hardware Trojan; Αξιοπιστία; Ηλεκτρομετανάστευση; Single Event Transient; Μεταβατικά Σφάλματα; Δίκτυο Τροφοδοσίας; Δίκτυο Δέντρο Ρολογιού; SET-triggered; Διεύρυνση παλμού; Benchmarks.

Table of contents

List of figures

List of tables

Abbreviations

ASCII	American Standard Code for Information Interchange
ATPG	Automatic Test Pattern Generation
BC	Boundary Condition
BE	Backward-Euler
BT	Balance Truncation
CUT	Circuit Under Test
DCT-II	Discrete Cosine Transformation of type-II
DD	Dual Damascene
EKS	Extended Krylov Sybspace
EM	Electromigration
FDM	Finite Difference Method
FIT	Failures In Time
GLP	Glitch Latching Probability
HT	Hardware Trojan
IC	Integrated Circuit
IDCT-II	Inverse Discrete Cosine Transformation of type-II
IP	Intellectual Property
LTI	Linear Time-Invariant
MM	Moment Matching
MOR	Model Order Reduction
NBTI	Negative Bias Temperature Instability
ODE	Ordinary Differential Equation
PDE	Partial Differential Equation
SA0	Stuck-at-0
SER	Soft Error Rate

SET	Single Event Transient
TTF	Time-to-Failure

Chapter 1

Introduction

1.1 Thesis contribution

This thesis discusses hardware security and its impact to reliability issues created in the ICs, if exploited accordingly. It's a subject not researched enough, as of today, in the scientific community, yet pairing security attacks with reliability issues can be a deadly combination. Physical effects, like Electromigration (EM) and radiation-induced transient faults, can severely disrupt the ICs' stability and performance. Any attack exploiting and aggravating these phenomena can accelerate or magnify the phenomena, depending on which reliability issue it focuses on. Although both the industry and the research community have exhaustively researched the subject of reliability closure and great advances have been made, both from the scientific community and the industry, it does not take into consideration yet the possibility of hardware attacks. This is because usually the community dealing with IC's reliability issues is not familiar with the hardware security threats and on the other hand attacks exploiting reliability phenomena are not established yet in the hardware security community. Thus, the ICs are deemed reliable and safe only under the specifications set by the designers, overlooking the probability a hardware attack has altered the design and manipulated reliability issues for malicious and destructive reasons. [1]

The research presented here focuses on the prevention of a hardware attack and the creation of challenging benchmarks for further aiding the effort of detecting reliability-based hardware trojans. For the prevention, an efficient methodology for checking the segments of a power grid for the most vulnerable ones to an attack is suggested to be integrated into the EM reliability sign-offs. As far as the creation of benchmarks is concerned, two algorithms are

introduced. The first one entails presenting a hardware trojan accelerating the EM phenomenon and locating the most optimal point on any gated clock for it to be inserted. The second, describes the design and function of a trojan that is triggered from a Single Event Transient (SET) and that ensures its propagation and the creation of a soft error.

1.2 Related Work

1.2.1 Hardware Security and Trojans

Nowadays, industries delegate the designing and fabrication of their ICs to third-party semiconductor fabrication plants to reduce production costs [2]. This practice has opened the door for individuals to infiltrate and add any malicious logic to the design. These extra components are called Hardware Trojans (HTs) and aim to inject faults to the proper function of the chip, leak sensitive information, like a cryptography key or the message to be decoded, or fully impair the chip and shut it down [3,4,5]. The result of their malicious output is called the *payload* of the Hardware Trojan (HT).

A successful trojan, other than achieving the intended attack, would be discrete and stealthy, meaning that the impact of its presence and activity should be as minimal as possible. Other than the case where the HT's purpose is to halt IC's functionality in full, the payload should not be able to be observed from the output of the design for it would be detected during the functionality tests after fabrication. Apart from the effect on the output of the chip, an HT's designer has to take into consideration its impact on the side-channel parameters, namely its power consumption, timing fingerprinting, thermal profiling, and leakage power. One way these can be circumvented is by adding a *trigger* to the trojan, designating a rare condition as its activation mechanism. Until the condition is met the HT remains dormant thus reinforcing its stealthiness. Triggers are not a necessary component of HTs, some may intend to steadily and continuously affect the IC over time while concealing their activity as a product of natural process variation. [6]

As it can be surmised, HTs can be greatly diverse and quite varying from one to another. However, attempts have been made by the research community to consolidate a broad enough taxonomy of their characteristics so any possible HT design can be included and categorized to provide a concrete guideline on countermeasures and detection techniques for each of them.

Taxonomy of HTs

In [7], a description of the hardware trojans was provided by the authors based on their physical characteristics, their payload as well as their activation conditions. Although trojans evolve and change day by day depending on the purpose of the attacker, the taxonomy presented establishes their fundamental characteristics to incorporate any new threat and assist in solidifying the detection and countermeasure techniques applicable to each category.

Under the category **physical characteristics** 1.1(a) fall the actual *size* of the HT's logic, the place of its insertion and whether its placement will lead to changes in the design's physical layout, referred to as *distribution* and *structure* respectively. The last subcategory, *type*, distinguishes between *parametric* trojans that alter only the intended logic of the IC and *functional* trojans that add extra gates and wires to the chip.

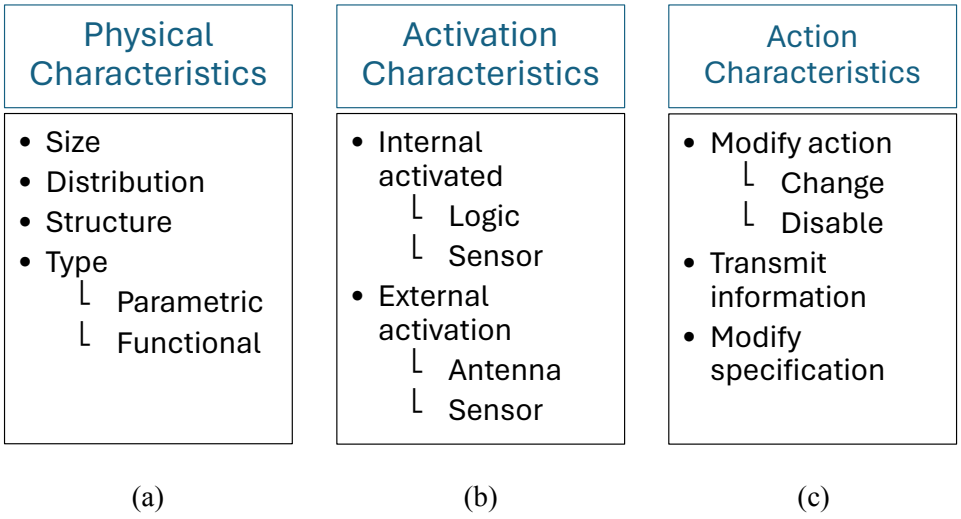


Figure 1.1: Taxonomy of HTs based on physical (a), activation (b), and action (c) characteristics.

The next category, **activation characteristics** 1.1(b), differentiates between the possible types of the trigger. *Internally activated* either needs a *condition*, usually rare, originating from the internal *logic* or a *sensor* for the HT to start its malicious operation, or it is set to be *always on* as long as the chip is on. An *externally activated* trigger would need a signal from the environment outside of the fabricated IC to start functioning incoming to an *antenna* or a *sensor*.

Last but not least, **action characteristics** 1.1(c) describes the payload of the trojan. The *modify function* category forks to *changing* the expected output of an operation and to the

total *disabling* of the chip, while in some designs, e.g. used in cryptography, *transmitting information* like the key is a valuable advantage to an attacker. The final subcategory is *modify specification* which, as the name suggests, results in altering the design's original specifications in order to disrupt the intended functionality of the IC.

Pre-silicon Countermeasures and Detection techniques of Hardware Trojans

Plenty of countermeasures and detection techniques have been developed since the topic of Hardware Security has been a research interest in the scientific community for over a decade. Both aim to confirm that the fabricated circuits under test (CUTs) have not been maliciously tampered with, however, countermeasures are applied before the fabrication stage of the production cycle. On the other hand, detection techniques are used after the fabrication of the circuits along with the post-silicon validation and testing.

Pre-silicon countermeasures techniques include designing-for-security, logic obfuscation, hardware watermarking, and even split manufacturing [8] to name a few. Split manufacturing is the simplest solution against the threat but the most costly. Delegating different components of the final design to individual fabrication foundries ensures greater security against HT insertion, however, it entails employing more than one foundry as well as the additional process of assembling the components to the final product by the designer company [9, 10].

Hardware watermarking is mainly used to protect Intellectual Property (IP). Watermarking applied in either the electronic system or in high-level synthesis level entails embedding the programmer's signature like timing and design constraints not already included in the specifications as a binary bitstream of American Standard Code for Information Interchange (ASCII) characters [11]. Another approach would be the triple-phase watermarking proposed methodology in [12]. The signature is applied during the high-level synthesis stage as well, however, it is split and the characters are distributed and checked during the scheduling, hardware allocation, and register allocation phase.

In a similar line, the main idea behind logic obfuscation techniques is inserting extra logic in the design, whose sole purpose is checking whether a specific obfuscation key is applied. When the correct one comes through, the function goes on as intended, otherwise, the design is ”locked” and a malfunction happens during the operation. This is achieved either by including XOR, XNOR and MUX-based logic locking [13] or by appending to the FSM states that are the previous states of the desired one but require the correct obfuscation key

to make the transition [14].

Design-for-trust also adds circuitry apart from gates for the intended functionality of the IC during the RTL coding phase. The purpose of these additions is to facilitate the survey of fabricated chips for any HT present. They can be ring-oscilators [15], current sensors [16], or dummy flip-flops [17] . The first two monitor the chip while it is active and spot any HT, the latter observe and control the internal gates of the chip to provide sufficient inputs to trigger the Trojan.

Detection techniques of Hardware Trojans

Although countermeasures help prevent the insertion of an HT in the design, not all cases and possibilities can be taken into consideration. Inspecting the fabricated chip for any malicious logic complements any design-for-trust already utilized. The most direct and invasive method involves deconstructing the chip and verifying the logic found at every layer. However, the drawbacks are that it is time-consuming, the chip itself is irreversibly damaged and there is no guarantee that the rest of the chips are trojan-free, even if the CUT is found clear [18]. As a result, non-destructive methods to check the chips are the main concern of the scientific community.

To begin with, logic testing methods observe any malicious activity on the output of the design, usually by producing uncommon test patterns as input to increase the probability of the HT being triggered [19]. However, that is possible in the event where the payload of the HT affects the output of the chip and simultaneously the design is small enough and, as a result, efficient in only a small number of HTs as well as supplementing other detection techniques [20]. For example, techniques that include an automatic test pattern generation (ATPG) method to find rare conditions that may be the trigger of the HT [21], or that add or manipulate existing scan-chain to either help activate the trojan [17] or partition the design so only one segment at a time is active to reduce noise during the main detection technique [22].

The most prominent methodologies, currently, include analyzing side-channel parameters such as power consumption, voltage, timing, and thermal profiling [23, 24, 25, 26]. Their main premise is to measure the corresponding parameter and verify it is under the expected threshold or exceeds it, suggesting the presence of extra logic in the CUT. The threshold can be obtained either from a Golden Chip, meaning a chip that is guaranteed trojan-free, from simulations, run in the finished design before it is sent for fabrication, or from measurements

taken from the CUT itself in different time frames. The challenge of these techniques lies with the naturally occurring process and environmental variations [27,28]. When a deviation from the expected measurements arises, it needs to be correctly categorized either as a threat or as a process variation.

1.2.2 Reliability issues and Hardware Security

One, currently not thoroughly explored, side of hardware security is the exploitation of reliability phenomena, such as EM and radiation-induced Single Event Transient (SET) pulses. The smooth operation of an IC is intrinsically connected to the reliability of an IC, so attacks targeting it accelerate and heighten the probability that related issues occur [1]. These attacks employ reliability hardware trojans, which range from modifying an existing wire in the design during manufacturing to injecting additional malicious logic into the chip, that focuses on aggravating the chosen reliability phenomenon and, thus, shortening the life of the IC or introducing faults to the intended operation [29,30].

Electromigration is the phenomenon caused by the continuous flow of high current passing through the wire. During its lifetime, two forces namely $F_{\text{electron-wind}}$ and $F_{\text{back-stress}}$ are applied on its metal atoms as shown in Fig. 1.2. The former is created from the flow of the current and the latter is an electrostatic force in the opposite direction, however, it is negligible to the first one [31]. As a result, the metal atoms accumulate on the anode creating compressive stress and hillocks, whereas on the cathode tensile stress and voids are formed. Over time, there is a change in the metal geometry, increased resistance, and open circuits shortening the wire's Time-to-Failure (TTF) and thus, the chip's overall lifetime.

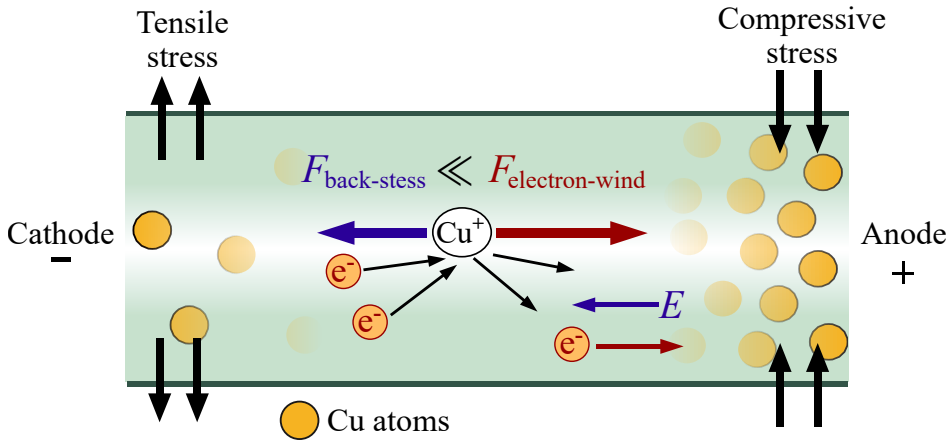


Figure 1.2: The forces in a metallic wire creating voids and the EM phenomenon. [2]

Single Event Transient, on the other hand, faults are the result of radiation hitting the IC's transistors. The source could be radioactive impurities in the package of the chip [32], and most importantly terrestrial cosmic rays that include high-energy neutrons [33]. That by itself is non-destructive. The hazard stems from the possibility that a pulse is created, due to the electron-hole pairs formed in the transistor's depletion region. The pulse is then propagated through the design and if it is caught from a memory cell, a soft error is created. Soft errors may lead from a temporary fault to a permanent malfunction depending on the memory element it altered. The vulnerability of the design to soft errors is depicted by the Soft Error Rate (SER) and is greater on modern IC due to the downscale of the technology [34,35].

Hardware attacks exploiting the aforementioned reliability issues would target the power grid, an interconnect, or a memory element whose failure would impact the performance of the design. A SET-based attack would entail adding radiation-sensitive logic to heighten the probability a pulse is generated and propagated to the rest of the logic [36]. These attacks are extremely challenging since their trigger is not able to be reproduced during the post-silicon testing of the chip. That would require emulating years of operation to observe any security threat benefiting from EM and continuously hitting the chips with radiation to detect the harmful logic. Thus, it is important to advance the research on detecting these types of attacks and so in this thesis, to further aid this endeavor, two methods to create HT-injected benchmarks for properly evaluating any detecting techniques and a Design-for-Trust method to be applied during the designing phase of the IC production.

1.3 Thesis organization

The remainder of the thesis is organized as follows: Chapter 2 gives a more detailed explanation of the modeling of the EM and SET faults phenomenon. Chapter 3 presents the methodology for an efficient security closure on power grid structures against an EM-base attack on them and Chapter 4 discusses an optimal methodology for EM-based Hardware Trojan placement on clock tree networks, as well as its most basic structure. Chapter 5 talks about a sensitivity-aware Hardware Trojan injection algorithm for Single Event Transient (SET) propagation and soft error attacks. Lastly, Chapter 6 concludes this work and mentions any possible future steps in this research.

Chapter 2

Modeling the reliability phenomena

2.1 Modeling the Electromigration phenomenon

As mentioned before, EM is a natural phenomenon occurring in the wires of the IC due to the constant flow of electricity, which harms them in the long term. It originates from the $F_{\text{electron-wind}}$ and $F_{\text{back-stress}}$ forces on the metal atoms creating stress, voids, and hillocks points, on the wire and changing its TTF. To calculate the stress applied over time and model the EM phenomenon, Korhonen's physics-based Partial Differential Equation (PDE) for stress diffusion is most commonly used [37]:

$$\frac{\partial \sigma}{\partial t} = \frac{\partial}{\partial x}\left[\kappa\left(\frac{\partial \sigma}{\partial x} + \beta j\right)\right] \tag{2.1}$$

The equation includes several variables and coefficients. The stress diffusivity coefficient κ is defined as $D_a \mathcal{B}\Omega/(k_B T)$, where $D_a = D_0 e^{-E_a/k_B T}$ represents the diffusion coefficient. E_a is the activation energy, D_0 is the diffusivity constant, $\mathcal{B}$ is the bulk modulus of the material, k_B is Boltzmann's constant, and T is the temperature. The EM driving force β is given by $(Z^* e\rho)/\Omega$, where e is the electron charge, ρ is the electrical resistivity of the wire, Z^* is the effective charge number, and Ω is the atomic volume for the metal. The equation is a function of time t and spatial coordinate x.

2.1.1 Boundary Conditions

The above equation applies to single-segment wires. However, the reality of ICs is that their wires create a mesh both in power grids and in the components' interconnects, creating

the necessity to regard a wire as multi-segment. Thus, changes should be applied to transform the PDE Eq. 2.1 into a system of Linear Time-Invariatiant (LTI) Ordinary Differential Equations (ODEs) for multi-segment structures. Firstly, proper boundary conditions (BCs) need to be applied. Regardless of whether the analysis is on an interconnect or a power line the following BCs need to be met [38]:

BC1 – Stress Continuity

For every node n_i, that $s_1, ..., s_k$ segments of the wire meet, the stress at the node must remain continuous. So, if $\sigma_{s_j}\big|_{n_i}$ is the stress applied to the node n_i from segment s_j, then the following must upheld:

$$\sigma_{s_1}\big|_{n_i} = \cdots = \sigma_{s_k}\big|_{n_i} \tag{2.2}$$

BC2 – Preservation of flux

Korhonen's equation obeys the mass conservation law meaning that mass remains balanced despite all of its transportation in and out of the wire. With S being the total number of segments this balance is expressed as:

$$\sum_{s_k \in S} \iiint \sigma_{s_k}\, dx\, dw\, d\tau = 0 \tag{2.3}$$

BC3 – Zero total net flux

Following the same line of thinking, the sum of the atomic flux must remain zero for every and any point n_i of the segments. Meaning:

$$\sum_{s_k \in S_{n_i}} w_{s_k} \tau_{s_k} \left(\frac{\partial \sigma_{s_k}}{\partial x}\bigg|_{n_i} + \beta j_k \right) = 0 \tag{2.4}$$

where $S_{n_i} = \{s_1, ..., s_m\}$ refer to the segments of the wire, n_i are the junction points, $w_1, \ldots, w_m$ the width of the segments, $\tau_1, \ldots, \tau_m$ their thickness and $j_1, \ldots, j_m$ the current density flowing through them.

BC4 – Zero boundary flux

In order to maintain the mass conversion law at every endpoint n_i connected to a segment s_k, for that specific segment k the total atomic flux must be equal to zero:

$$\left(\frac{\partial \sigma_{s_k}}{\partial x}\Big|_{x=n_i} + \beta j_{s_k} \right) = 0 \tag{2.5}$$

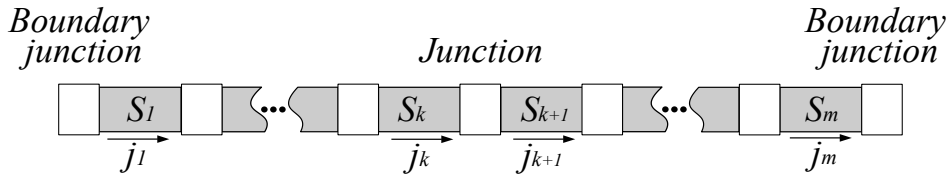


Figure 2.1: An m-segment interconnect line.

Fig. 2.1 shows an interconnect wire, segmented into m sections. If the power grid is made out of Cu DD technology, then each of its layers is electrically isolated from the next and previous one. This provides the advantage that power grids can be analyzed in lines, the same way as any other interconnect wire, without the need to perform EM analysis on the whole of the power grid [39].

2.1.2 Discretization and final equation for stress.

The next step in transforming Eq. 2.1 is to discretize every wire, for interconnects and power grid lines alike, uniformly into segments. This process is achieved using the Finite Difference Method (FDM). Then, combining the discretization process with the application of the aforementioned BCs, Korhonen's PDE is converted into a system of ODEs for calculating the stress over time $\sigma(t)$ [40]. The general form of the final system, that can be applied both for interconnect structures and for power grid lines is:

$$\mathbf{C}\dot{\boldsymbol{\sigma}}(t) = \mathbf{A}\boldsymbol{\sigma}(t) + \mathbf{B}\mathbf{j}(t) \tag{2.6}$$

where the number of the segments is defined by the parameter m, the discretization points are denoted as n, $\mathbf{C} \in \mathbb{R}^{n\times n}$ is the coefficient matrix of the EM stress derivative at each internal node of the system, $\mathbf{A} \in \mathbb{R}^{n\times n}$ is the coefficient matrix of the stress and $\mathbf{B} \in \mathbb{R}^{n\times m}$ is the matrix that maps the current densities to the stress at each internal node.

The Eq. 2.6 can be simplified for analyzing power grid structures, since in that case, matrix $\mathbf{C}$ is the identity matrix. Then, the system becomes:

$$\dot{\sigma}(t) = \mathbf{A}\sigma(t) + \mathbf{B}\mathbf{j}(t) \tag{2.7}$$

These models are used to simulate stress during sign-off for all the structures of the design to pinpoint the lifetime of the design and validate its EM-safe. If the stress surpasses the threshold of the critical stress, then voids and hillocks start to form and the structure is considered broken. The parameter t in Eqs. 2.6 and 2.7 specifies the period the structure would be active. The stress is calculated for the design's target lifetime stated in the specifications and the necessary changes are applied in the structure unless it is found EM-safe.

2.2 Modeling Singe Event Transient faults

As mentioned before, SET faults are soft errors that originate from high-energy particle hits on a sensitive region of a gate. Soft errors are defined as temporary and non-destructive errors to the design as opposed to hard errors that are permanent in the circuitry. Even though particle hits are a frequent occurrence in space, they have also been observed on terrestrial devices. These hits are generated either from emissions originating from low-concentrated impurities of the ICs' packaging materials, such as uranium and thorium, that over time decay [41], or from cosmic radiation colliding with atmospheric atoms and cascading until they reach sea level [42]. The former are alpha particles while the latter are energetic neutrons. Both of them may interact with the silicon nuclei in a chip and create electrical disturbances and thus potential soft errors.

There are two stages to properly model the transient faults [43]. The first one entails simulating the particle hit on the gate under test in order to figure out the angles of the hit and the respective energy the particle needs to carry for current to be created at the output of every gate in the design as well as the induced current and pulse. The second stage is simulating the propagation of the pulse throughout the rest of the circuit at various moments in a clock period, to evaluate whether a soft error would occur or not.

The probability that a transient fault originating at a gate's output will result in a soft error is used to evaluate gate sensitivity. After completing the simulations, combining the sensitivity of each gate contributes to the overall SER estimation of the design. The latter denotes whether the final design is reliable from the radiation-safe standpoint or whether radiation-hardening techniques need to be applied to mitigate the phenomenon. The following sections detail the methods used in the upcoming research to model SET faults, using the methodology developed in [44].

2.2.1 Particle hit and propagation modeling

A high-energy particle hit does not guarantee a current pulse is generated. For a transient fault to be generated the minimum charge caused by the particle's impact should be at least equal to the critical charge Q_{crit}. This metric is unique to each gate, it is solely related to the device characteristics, and as the technology continually shrinks its value decreases, meaning that particles of smaller energies can cause a malfunction in circuit operation.

The primary ways to simulate a particle hit and model the resulting additional current and transient pulse are by using either TCAD tools, e.g. Sentaurus, or electrical SPICE simulations. The latter is used in the methodologies that follow. The radiation-induced current is modeled by the double-exponential current pulse and is expressed for every moment in time of a clock period [45] as:

$$I_{particle}(t) = \frac{Q_{coll}}{\tau_\alpha - \tau_\beta}(e^{-t/\tau_\alpha} - e^{-t/\tau_\beta}) \tag{2.8}$$

where Q_{coll} is the collected charge at the gate, τ_α is the time moment the electron-hole pairs are deposited in the p-n junction, and τ_β is the time the particle hits the silicon. The former indicates the rise time of the current pulse and the latter equates to the fall time. Q_{coll}, contrary to Q_{crit} is determined by the characteristics of the device, the energy of the particle hit, and the angle. Utilising the integral of the calculated $I_{particle}$ with respect to time, the Q_{crit} is estimated:

$$Q_{crit} = \int_t^0 I_{particle}(t)\, dt \tag{2.9}$$

The next step, after the particle hit, is simulating the propagation of the generated SET pulse. As mentioned before, SPICE is used for the simulation to determine whether the pulse would reach a memory element. One important factor is the width of the pulse and its amplitude, making the SET pulse characterization a crucial process. In turn, these are affected by the strength of the particle [46]. The simulation itself entails choosing random transistors and at various time windows during the clock period induce current pulses and their spread through the rest of the design is examined. As a result, to accumulate accurate data several iterations of the simulation and characteristics of the pulse are performed. If a pulse reaches at least one memory element during the latching window, then it is considered to cause a soft error. For this reason, both setup and hold time for the memory elements are taken into consideration during the simulations.

This is one of the inherent masking mechanisms present in the circuit, specifically the timing masking mechanism. The other two that are present are the logical masking and the electrical masking. Both of them are taken into consideration and affect the propagation of the pulse [47]. The high number of simulations needed is to ensure these three mechanisms are explored sufficiently and thoroughly, even though the total runtime becomes high.

2.2.2 Gate sensitivity and Soft Error Rate

After all the simulations are done, all the necessary data have been accumulated to be able to compute the gate sensitivity and the SER. Gate sensitivity refers to the probability that a SET pulse generated at the gate's output will be latched by a memory element. This metric is different for every gate in the design and is denoted as Glitch Latching Probability (GLP). Each gate's probability is calculated and assigned during the simulations of the particle hits following this equation:

$$GLP = \frac{1}{n} \sum_{i=1}^{n} latched\_glitch(i) \tag{2.10}$$

where:

$$n = l \times e \times t \tag{2.11}$$

with n as the total number of simulations, l being the number of the different primary input vectors needed for including the logical masking mechanism, e denotes the number of unique width pulses, t is the number of the unique time moments that a soft error was created during the clock period and $latched\_glitch$ is either 1 or 0 depending whether a soft error occurred or not.

The SER metric corresponds to the total latching probability of the circuitry in its totality, meaning how sensitive the design is at a soft error occurring from a SET pulse. It is estimated for every iteration of the simulation and at the end the overall SER_{prob} is calculated. The semiconductor industry uses the Failures In Time (FIT) SER metric. SER_{FIT} specifies the soft errors occurring per one billion hours and is calculated using the equation:

$$SER_{FIT} = F \times A \times SER_{prob} \tag{2.12}$$

where F is the neutron flux and A is the area of the circuit under test, which is exposed to the flux.

This method, as was originally and more thoroughly presented in [44], is implemented for modeling a SET glitch generating, propagating, and calculating the associating metrics for deciding the level of reliability of the design. The methodology and the Eqs. 2.8 - 2.12 were also used in the ensuing research presented.

Chapter 3

An Efficient Security Closure Methodology for Electromigration-based Attacks on Power Grid Structures

3.1 Introduction

The increasing demand for performance and the continuous downscaling of structural dimensions pose an ongoing challenge to the reliability of these devices. Factors such as electromigration (EM) have emerged as significant risks for the reliability of modern chips [48]. Consequently, attackers are progressively utilizing reliability-based HTs to deliberately induce long-term consequences on the stability and performance of the IC. These malicious components are designed with the specific target of accelerating several reliability issues, such as premature aging or EM, in particular, interconnect regions of the IC [49]. Such effects can result in unexpected system behavior or even system downtime. To detect these types of attacks, the most established approach is the utilization of side-channel analysis methods. These methods rely on various parameters, including voltages, currents, and timing, to identify any anomalous or suspicious behavior in several regions of the chip [24, 25, 50].

Power grid structures play a critical role in the reliable operation of integrated circuits as they are responsible for distributing power to logic gates and maintaining overall functionality in VLSI designs [51]. To address the increased current within power grids and mitigate EM stress, substantial decoupling capacitances, acting like a reservoir, are added across multiple metal layers. These reservoirs consist of passive wire segments designed to enhance reliability

and robustness by providing greater resistance while minimizing impacts on performance and power consumption of the power grid structure [1]. While reservoirs are a crucial component of power grids, they are also susceptible to stealthy attacks that aim to reduce or remove the reservoirs from the power grid network of the design.

The integration of an efficient security closure methodology into industrial physical design flows is essential for assessing the functionality of power grids. Thus, an efficient methodology that utilizes a semi-analytical approach [40] to calculate the time-to-failure of each power grid line separately was developed. The algorithm discretizes only the spatial domain while keeping the time domain continuous and incorporates a binary search method to ensure fast convergence.

3.2 Decoupling capacitance in power grids

Technology nowadays has reached nanoscale dominion making signal integrity a serious issue, especially in power sources. The power grid of a chip connects with every element in the design, subjecting it to multiple switching activities within every clock period. The result of that is a considerable amount of noise to be created that affects the supply voltage distributed to the design, leading to logic failures, degradation of transistors, and lowering the reliability of high-performance circuits [52]. To help mitigate any voltage fluctuations in the power network decoupling capacitors (also known as decap) are added, acting as reservoirs. These are smaller capacitors that are placed in empty spaces close to the source of the noise.

Research around decaps includes pinpointing where they can be placed since enough space on the die is needed [53], and their capacitance size [54]. They can be used in the interconnects of the design in addition to the power grid, however on the latter, its effect is the most valuable since the power grid is responsible for the entirety of the design. Placing decoupling capacitors efficiently and deciding their size is an integral aspect of power grid optimization [55]. Thus, removing a decap from a finalized and developed power network would impact both its reliability and the general functionality of the design.

3.3 Hardware security and power grids

Any attacks aiming at exploiting EM would entail inserting a resistive element such as narrow wires, at a crucial interconnect point to increase the current flow and as a result, accelerate the creation of a void in that point of the attack. Attackers can strategically position these resistive elements within crucial circuit paths, such as clock tree networks, to create HTs that trigger specific system failures. These modifications, however, can be observed by side-channel analysis detection techniques.

Another option for keeping the attack stealthy is to remove or modify the decoupling capacitance structure, which work like reservoirs, within the power grid. These reservoirs are typically positioned at the cathode terminal of lines, as seen in Fig. 3.1, that are more prone to EM failures. More specifically reservoirs enforce the steady-state stress to remain below the critical stress, in order to make the power grid structure immortal to EM failures. By removing the reservoir, the EM stress on the line accelerates, leading to a stealthy degradation of the TTF well below the desired level.

Figure 3.1: An electromigration-based attack on an AND gate.

Another crucial aspect of the decap removal attack, which needs to be considered, is its minimal impact on the performance, power consumption, and IR drop of the IC, while effectively compromising the functionality of the power grid. This characteristic poses a significant challenge in distinguishing an attacked circuit's behavior from a legitimate one. Furthermore, in today's advanced technology nodes where the margins for EM safe design are narrower, the threat posed by these Trojans becomes even more concerning. Their impact can remain at the minimum, meaning they can remain undetected by various side-channel analysis methods. All of the above have made security closure methodologies a critical aspect of the physical design methodologies.

3.4 Security Closure Methodology for Reservoir Reduction Attacks

Detecting potential EM-based trojans in power grids poses a significant challenge in implementing an efficient security closure methodology. These Trojans can remain undetected by avoiding the generation of observable side-channel leakage measurements. Furthermore conducting comprehensive EM analysis for every potential scenario has become increasingly difficult since the number of metal lines in modern VLSI power grids has increased. In the proposed security closure methodology, we adopt an approach where each power grid line is individually analyzed.

3.4.1 Calculation of power grid's Time-To-Failure using binary search

An important part of the research is the calculation of the expected TTF. While the solution methodology is capable of independently computing the EM stress at each time stamp, it cannot determine the TTF beforehand. To determine the TTF, the methodology requires the specification of a time interval denoted as $[t_{min}, t_{max}]$. This interval serves as a

Algorithm 1 Calculation of TTF based on the rightmost binary search.

Input: t_{min}, t_{max}

Output: time to fail TTF

$t_{left} = t_{min}$, $t_{right} = t_{max}$

while $t_{left} < t_{right}$ **do**

  Set the new time stamp $t_{mid} = floor((t_{left} + t_{right})/2)$

  Calculate the EM stress at t_{mid} by employing the analytical method.

  if $\sigma(t_{mid}) > \sigma_{critical}$ **then**

    $t_{right} = t_{mid}$

  else

    $t_{left} = t_{mid} + 1_{year}$

  end

  $TTF = t_{right}$

end

reference for identifying the specific time stamp at which the power grid reaches the critical stress level $\sigma_{critical}$, thereby indicating the TTF. Following the determination of the time

interval, a rightmost binary search approach is employed within this interval, as shown in Alg. 1. This involves repeatedly calculating the EM stress at selected time stamps such as:

$$t_{mid} = \textit{floor}((t_{left} + t_{right})/2)$$

until convergence is achieved. Convergence is considered to occur when the calculated stress matches the critical stress value of the technology. This iterative process ensures the accurate estimation of the expected TTF for the power grid structure. The complexity of the binary search algorithm is $\mathcal{O}(\log t)$, where t represents the length of the time interval. However, it is worth noting that the time intervals involved in power grid analysis are typically tight and rarely exceed 100 years. Therefore, the overall computational complexity remains manageable and still can be performed independently for each power grid line.

3.4.2 Methodology for removing the decaps

With an efficient algorithm for computing the TTF of the design developed, the rest of the methodology is presented. First, each of the power grid lines is extracted separately and the FDM discretization is applied on each line, as described in [56]. By discretizing each line only the spatial domain using FDM, while keeping the time domain continuous, we can construct the systems of equations like Eq. 2.7. This parallel approach allows us to effectively model and analyze the behavior of the power grid, enabling accurate assessment and evaluation of its reliability.

Once the equation systems are formulated, we employ an efficient semi-analytical solver, which was proposed in [40], specifically designed for systems resulting from FDM spatial discretization on power grid line structures. This approach leverages the unique tri-diagonal structure of the resulting system matrix $\mathbf{G}$ which easily tracks Fast Poisson solvers [57] and leads to the following closed-form matrix equation:

$$\boldsymbol{\sigma}(t) = \mathbf{V}\mathbf{L}(t)\mathbf{V}^T\mathbf{B}\mathbf{j} \tag{3.1}$$

where:

$$\mathbf{L}(t) = \begin{bmatrix} t & & & \\ & \frac{e^{\lambda_2 t}-1}{\lambda_2} & & \\ & & \ddots & \\ & & & \frac{e^{\lambda_n t}-1}{\lambda_n} \end{bmatrix} \tag{3.2}$$

with $\mathbf{V} \in \mathbb{R}^{n \times n}$ is the matrix containing the eigenvectors of matrix $\mathbf{A}$ and λ_i with $i \in [1, n]$ are the corresponding eigenvalues. The fundamental advantage of this method is that once the Eq. 3.1 is constructed, then the stress can be easily computed by substituting the desired time stamp t into the equation.

An important aspect of this method is that utilizes the unique tri-diagonal structure of matrix $\mathbf{G}$ to take advantage of fast Poisson solvers, enabling the determination of eigenvalues and eigenvectors in advance. Specifically, the operations of multiplying matrices $\mathbf{V}^T$ and $\mathbf{V}$ with vector $\mathbf{r}$, denoted as $\mathbf{V}^T\mathbf{r}$ and $\mathbf{Vr}$, respectively, perform a Discrete Cosine Transform of type-II (DCT-II) and an Inverse DCT of type-II (IDCT-II). By employing these transformations, the computational complexity of matrix multiplication is reduced from $\mathcal{O}(n^2)$ to $\mathcal{O}(n \log n)$. This solution offers a straightforward and easily parallelizable closed-form equation that can be independently applied to each different power grid line, efficiently computing the EM transient stress for a given time t in near-linear time.

Algorithm 2 Security Closure Methodology for Power Grid Structures

1: Extract the power grid network from the design.
2: Construct the corresponding discretized system to calculate the stress of each line.
3: Set the analysis interval $[t_{min}, t_{max}]$ to perform the TTF calculation of each line.
4: For all the lines in parallel perform binary search of Alg. 1, TTF=`bs_right_most`(t_{min}, t_{max})
5: Determine the susceptible lines of the power grid design.
6: Report all the corresponding TTFs with and without reservoirs of the susceptible lines.

After computing the TTF for each power grid line, Algo. 1, our methodology identifies the susceptible lines. These susceptible lines are the ones that would become vulnerable and fail in the event of a potential EM-based Trojan attack that involves reservoir removal. By detecting these susceptible lines, our methodology provides valuable insights into the critical points within the power grid structure that are prone to such attacks. Furthermore, the proposed method reports the TTF with and without the presence of decaps, which helps in understanding the impact of reservoir removal on the reliability of the IC. This information enables proactive measures to enhance the security and reliability of the IC, allowing for the implementation of targeted countermeasures to protect against EM-based Trojan attacks.

Since our methodology performs exhaustive simulations on the power grid lines that are more susceptible to the creation of EM hotspots, the power grid network can be considered

EM-safe if the reservoir removal attack does not result in the failure of these lines. The important steps of our method are summarized in the Alg. 2,

3.5 Evaluation of the methodology

3.5.1 Experimental setup

In order to validate the efficiency and the effectiveness of our method, we have conducted experiments on several large-scale power grid benchmarks from OpenROAD project [1]. These benchmarks were implemented using different technologies, including a commercial 12nm FinFET, commercial 28nm FDSOI, and Nangate 45nm libraries. For our evaluation, we have employed the BFS traversal algorithm to extract the multi-segment interconnect lines from these benchmarks, with the critical stress level set to 50MPa [39]. The TTF specification of the benchmarks was set at 20 years, which is a commonly targeted lifetime in processor design. Algorithms 2 and 1 were implemented in Python using the scientific computation library Scipy. For all experiments, we conducted the evaluation on a Windows workstation with a i9-9900K processor of 16 threads and 32GB RAM memory.

Table 3.1, demonstrates the characteristics of the benchmarks prepared for our algorithms to be implemented on them. Specifically, column *#Lines* reports the number of extracted lines for each benchmark, while the *Dscr. step* indicates the discretization step of the spatial coordinate. The *Avg. #Discr. points* refers to the average number of discretization points used in constructing the ODE system. Last, column *Min. TTF (yrs)* reports for each design its lifetime with all the decaps in the power grid network.

3.5.2 Assesment of the experimental results

After the construction of the corresponding discretized system, the next big step in Alg. 2 is to implement the binary search, Alg. 1, to calculate the TTF with the reservoirs, find the susceptible lines of the power grid and re-calculate the TTF without the decaps, which is the bulk of the time-consuming process and the part the latter algorithm improves. The totality of the results is shown in Table 3.2. Column *#Lines* is reported again for easy comparison to column *#Susceptible lines* that displays the total number of lines with a TTF less than the

[1] Github repository: `https://github.com/The-OpenROAD-Project`

Table 3.1: Characteristics of the benchmarks

Tech	Design	#Lines	Discr. step (m)	Avg. #Discr. points	Min. TTF (yrs)
45 nm	dyn_node	1402	0.15	2535.86	37
	ibex	697	0.19	2754.63	32
	aes	1182	0.18	2897.01	35
	jpeg	3505	0.14	3003.14	38
	swerv	5413	0.13	3075.06	30
28 nm	gcd	191	0.78	7291.04	34
	aes	46	0.80	1626.13	37
	jpeg	406	0.76	18875.74	38
12 nm	gcd	110549	0.02	10689.25	27
	ibex	86024	0.02	10665.49	31
	jpeg	2375	0.05	10355.66	37
	dyn_node	12472	0.03	10549.42	58
	aes	47603	0.02	10653.08	56

expected 20-year lifetime after removing the reservoir.

Additionally, the minimum TTF in years with decaps is restated for comparison with subcolumn *No Decap* that holds the respective results. Their difference is calculated in column *Avg. Diff. TTF (%)* for ease. Last but not least, the robustness of Alg. 1 is shown in column *Largest Line* that informs the total time in seconds for the execution runtime and how many segments, for reference, the line has.

As demonstrated in Table 3.2, the developed method effectively identifies the susceptible lines, which are considerably fewer in number compared to the total lines of each benchmark. This presents a significant challenge for any side-channel analysis techniques aiming to detect HTs. Furthermore, it is worth noting that the TTF of the lines has been significantly reduced

Table 3.2: Experimental results of the methodology for large-scale OpenROAD power grid benchmarks

Tech	Design	#Lines	#Susceptible lines	Avg. Diff. TTF (%)	Min. TTF (yrs)		Largest Line	
					With Decap	No Decap	#segs	Total time (s)
45 nm	dyn_node	1402	15	50.39	37	12	243	8.78
	ibex	697	28	29.63	32	14	229	5.66
	aes	1182	18	52.81	35	11	320	12.25
	jpeg	3505	12	50.43	38	13	550	30.29
	swerv	5413	14	51.81	40	14	597	32.03
28 nm	gcd	191	14	58.72	34	9	478	3.68
	aes	46	8	40.51	37	11	121	0.13
	jpeg	406	10	50.58	38	11	961	14.60
12 nm	gcd	110549	16	54.82	27	13	1360	26.79
	ibex	86024	18	41.64	31	16	1312	29.81
	jpeg	2375	9	48.15	37	13	220	0.67
	dyn_node	12472	12	63.55	58	13	496	4.71
	aes	47603	11	36.17	56	14	979	16.38

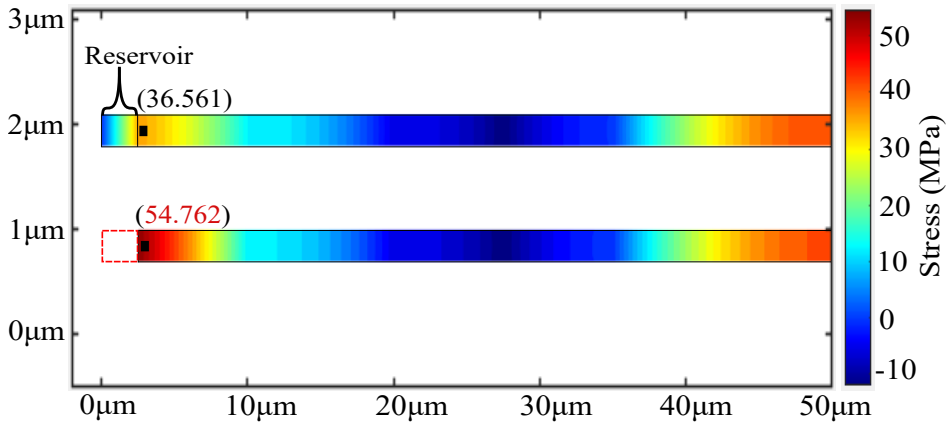


Figure 3.2: EM stress build-up at t = 20 years for a 74-segment line from the *45 nm aes* design.

by up to 63%, with a minimum expected lifetime of 9 years.

Furthermore, our methodology can be executed entirely in parallel for different lines, with the execution time dominated by the largest line. In this regard, the table reveals the impressive efficiency of our approach in conducting EM analysis, even for the worst-case scenarios, as evidenced by the runtimes of the largest lines.

Finally, Fig. 3.2 and Fig. 3.3 demonstrate the stress build-up for a 74-segment line from

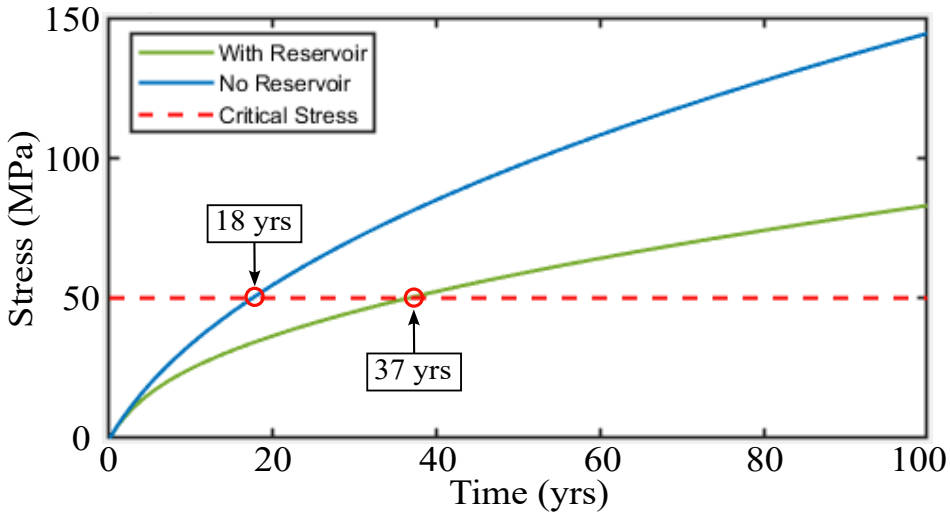


Figure 3.3: Transient simulation of the attack point for a 74-segment line from the *45 nm aes* design.

the 45 nm aes design, with and without the presence of a reservoir. In particular, Fig. 3.2 depicts the overall stress accumulation at $t = 20$ years, while Fig. 3.3 specifically focuses on the stress waveforms at the attack point of the line. As can be seen, the attack point surpasses the critical stress level earlier, resulting in a reduced TTF of the line to 50%. These figures visually demonstrate the impact of reservoir removal Trojan attacks on the stress distribution and highlight the importance of reservoirs in maintaining the desired TTF of the power grid line.

Chapter 4

An Optimal Methodology for EM-based Hardware Trojan Placement on Clock Tree Networks

4.1 Introduction

Since the fabrication of ICs is nowadays delegated to third-party foundries to cut down on costs, an important step of Hardware Security is to test the fabricated chips for any HT presence. Generally, Hardware Trojans aim to exploit the IC's characteristics to insert faults. Reliability issues, such as the Electromigration phenomenon, are prime candidates to be exploited since they affect the general stability and performance of the IC. Reliability HTs consider these vulnerabilities for the foundation of their design, functionality, and payload. Specifically, Electromigration-based Hardware Trojans aggravate the already present EM phenomenon on the interconnects they target [49].

Even thought various detection techniques are being developed currently, as already mentioned in 1.2.1, a reliable evaluation of these techniques is intrinsically connected to the quality of the benchmarks they are tested on. Evaluating the effectiveness of the detection algorithms is as vital as the algorithms themselves. So, to further aid this endeavor we developed an algorithm for finding the most optimal place to insert an Electromigration-based Hardware Trojan (EM-based HT) in a gated clock tree network. [1]

Generally, trojans aim to exploit the IC's characteristics to insert faults. Reliability issues, such as the EM phenomenon, are prime candidates to be exploited since they affect the

general stability and performance of the IC. Furthermore, advanced process nodes are used for the chip's fabrication so they consist by themselves an important risk for the IC [48]. Reliability HTs take these presented vulnerabilities into consideration for the foundation of their design and functionality. Specifically, EM-based HTs focus on aggravating the already present phenomenon on the interconnects they target [49].

In this paper, an optimal strategy for EM-based HT benchmark creation for clock tree networks is proposed. The main contributions of this paper are summarized as follows. First, it efficiently searches the clock tree network of the design under attack to locate the place where the reliability-based HT would be injected in a stealthy manner, making it undetectable through side-channel analysis measurements. Second, the proposed placement strategy can be readily adapted to clock-gated designs. Last, the fact that EM stress is more pronounced in vias and junctions of interconnects is leveraged to accelerate the methodology by using a Model Order Reduction (MOR) approach [38]. The presented algorithm is evaluated by using a set of clock tree networks derived from microprocessor designs with random control logic and datapath.

4.2 Gated clock tree networks

The clock tree networks are responsible for synchronizing and facilitating the smooth operation of the whole of the chip. This renders them a vulnerable component for placing an EM-based HT. The clock tree reaches the entirety of the IC and is always active, so it has a high frequency and high average current flowing through its interconnects, and as a result, is subjected to constant EM stress. However, gated clock tree networks have been suggested by the research community, primarily to mitigate their overall power consumption [58, 59].

A gated clock tree network is activity-driven, meaning there is control logic that, paired with an enable signal, activates or deactivates part of the clock tree depending on the needs of the current cycle [60]. So, not all of the clock nets get the same amount of stress and therefore, some of them are not as vulnerable to failure due to EM as others. Adding sufficient stress to not EM susceptible nets via a reliability Trojan, to push them beyond the critical threshold, would make the Trojan less stealthy and more susceptible to detection. Thus, the placement of the Trojan on the clock tree networks should be taken into serious consideration to achieve maximum impact on the VLSI design while remaining properly concealed [61, 62].

4.3 Electromigration based Hardware Trojans

A Hardware Trojan alters the behavior of the design it is inserted into in a malicious way. Electromigration-based Trojans target the reliability of ICs since they play an important role in the stability and performance of an IC. It accelerates the phenomenon, by increasing the local current density of an interconnect and leading to its premature failure. This is achieved by adding resistive elements, such as a narrow, more susceptible to the Electromigration phenomenon, wire, in the critical paths of an IC. In this case, a critical path does not refer to the path with the worst delay or the longest, but rather the path whose failure would spread a fault to the majority of the IC or one of its crucial functionalities.

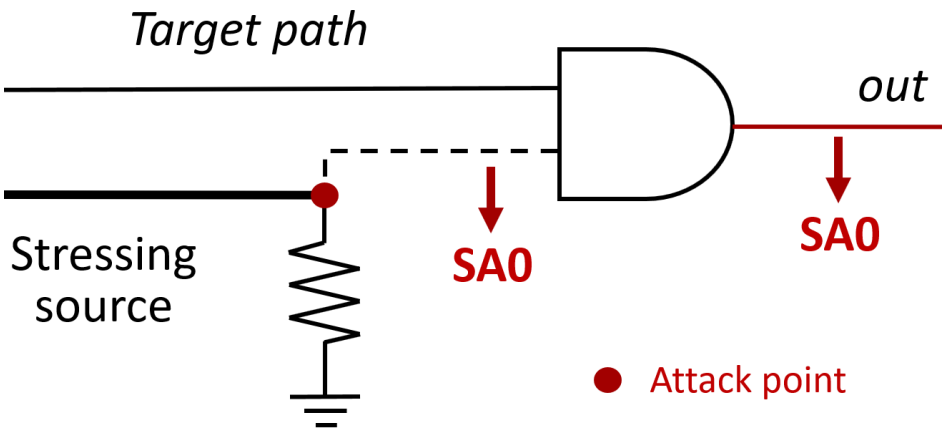


Figure 4.1: An electromigration-based attack on an AND gate. [1]

The simplest circuit constituting an Electromigration-based Hardware Trojan is shown in Fig. 4.1 [49]. The goal is to add to the current density flowing through the Trojan wire to increase the stress. For this purpose, a resistor is added that leads to a ground node, completing a circuit and providing supplementary, constant, current flow. As aforementioned, an added resistor constitutes the simplest EM-based attack. However, any other circuit or structure injected having the same effect falls in the same category, making EM-based HTs as diverse as any other type of HT.

The Trojan in Fig. 4.1 manipulates the attacked interconnect's logic value to be stuck-at-0 (SA0) after the successful attack, exploiting the EM phenomenon. This can be used as a trigger to target a path of the IC that includes an AND gate. The intended functionality of an AND gate is shown in Table 4.1. However, after the Trojan wire's insertion, the input interconnect's natural aging effects on the attack point accelerate. Ultimately, it fails causing

the input to the AND gate to be SA0 changing its functionality as shown in Table 4.2 and affecting any circuit using the *out*'s logic value. The impact of the attack becomes greater if the attack point is located on an *enable* signal since the injected fault renders every component lead by the AND gate permanently inactive.

Target path	Trojan wire	*out*
0	0	1
0	1	0
1	0	0
1	1	1

Table 4.1: AND's truth table before the attack.

Target path	Trojan wire	*out*
0	0	1
0	0	0
1	0	0
1	0	0

Table 4.2: AND's truth table after the attack.

HTs intend to remain stealthy and undetectable from any side-channel analysis techniques, the leading methods for HT detection currently in research. These techniques observe any voltage or current variations on the circuit under test (CUT) that can be attributed to the presence of an HT while ensuring these variations do not occur from the natural process variations in an IC [27, 28]. However, an EM-based Hardware Trojan may need additional components inserted into the IC to ensure that the trojan wire will be sufficiently stressed, which might have an impact on the power consumption of the IC. Thus, making the design and placement of an EM-based Hardware Trojan challenging. The attacker can leverage the IC's designed components to hide the attack behind the circuit's normal activity while aggravating the EM phenomenon at the attack point. Furthermore, to further solidify its stealthiness, the trojan must introduce the minimum current possible to achieve the desired Time-To-Failure (TTF), so that the power consumption difference to be masked by the natural process variations.

4.4 Model Order Reduction using the Extended Krylov Subspace Moment Matching method

The designers of chips simulate their design to analyze its functional behavior, optimize it, and ensure the overall design's stability, and reliability, and that its constraints are met

before fabrication occurs. Nowadays the high complexity of the VLSI designs makes their modeling and simulation computationally expensive as far as time and memory storage are concerned. Fortunately, the original system can be reduced to a smaller one with Model Order Reduction (MOR) techniques, whose functionality at the input-to-output ports is similar to the original design. They generate a dynamical smaller system that has identical functionality as the original one in the frequency range of interest [63, 64, 65].

Model Order Reduction methods are divided into two major categories: System Theoretic and Moment-Matching (MM). The former includes methods such as Balance Truncation (BT), which achieves better precision of the approximation error but demands high memory storage and computational costs. The latter ensures lower computational costs, however, they may not reach a sufficiently reduced order or be as accurate since the approximation error cannot be estimated beforehand [66, 67].

Moment Matching techniques are used to model accurately the signal delays for the reduced model through the design, based on the original design's characteristics. These methods, calculate and choose moments of the spectrum that constitute the subspace of the original system to generate the reduced model so that it maintains identical functionality and behavior as the initial. This means that when these moments are used to expand the reduced model, they will produce a system matching the one calculated from [68]. Many methodologies in the last three decades have been proposed for constructing this subspace [69, 70, 71], one of the most established ones utilize the standard Krylov Space [72, 73, 74, 75].

In [65], the authors extended these the MM techniques by applying the Extended Krylov Subspace (EKS) instead of the standard Krylov Space, for the creation of the subspace. The evaluation of the method shows a significantly greater accuracy achieved of the produced reduced model, almost eliminating the MM technique's drawback. Specifically, the new subspace is defined as the projection matrix V consisting of the standard Krylov subspace [76, 77] $\mathcal{K}_k(\mathbf{A}_E, \mathbf{B}_E)$ with the extension to include the inverse $\mathbf{A}_E^{-1}$ resulting in:}

$$\mathbf{V} = \text{range}(\mathbf{V}) = \mathcal{K}_k(\mathbf{A}_E, \mathbf{B}_E) + \mathcal{K}_k(\mathbf{A}_E^{-1}, \mathbf{B}_E) \tag{4.1}$$

where

$$\mathbf{A}_E \equiv \mathbf{A}^{-1}\mathbf{C}, \quad \mathbf{B}_E \equiv \mathbf{A}^{-1}\mathbf{B}$$

Thus, creating and utilizing the EKS to minimize the disadvantages of the MM technique. It introduces a small overhead in the calculation expenses but still requires overall less than

the equivalent of the BT technique.

4.5 The optimal Electromigration-based Trojan placement algorithm

Combining all of the above in [1], an algorithm was developed for placing EM-based reliability HTs in any gated clock tree network and creating challenging benchmarks for satisfactorily evaluating any side-channel analysis identification technique. It is vital to be aware of the extra current introduced when deciding the insertion point. It should be enough to accelerate the EM phenomenon on the target point of the wire to achieve the desired TTF while remaining under the threshold of being masked as the naturally occurring process variations of the fabricated IC. Any excessive current introduced, on the one hand, would make a bigger number of interconnects suitable for placement, on the other hand, would have a greater impact on the consumption of the power and current in the IC, making the HT susceptible to be detected by the side-channel analysis methods.

Assessing the EM susceptibility of the clock tree is the first step in our methodology. EM analysis dictates each wire be discretized into segments and, for each one of them, calculate its EM stress based on the design's lifetime specification. As it can be surmised, this process for each segment of each wire of the clock tree covering the entirety of an IC is both time and computational consuming. However, research in [78] shows that vias and blocking points in the interconnect are more vulnerable to voids due to EM phenomenon. Performing transient analysis on these regions reveals a peak in the stress function at these points, confirming that argument [79, 80]. Thus, only those points can be analyzed by excluding the rest through a MOR process, reducing the resources and the simulation time needed without losing any accuracy. Specifically, in our methodology, the MM EKS technique was applied. In order to start the process, we need to define the matrix $\mathbf{L}$ as:

$$\mathbf{y}(t) = \mathbf{L}\,\sigma(t) \tag{4.2}$$

where $\mathbf{y} \in \mathbb{R}^q$ is a vector containing the EM stress at the monitor points, with q being the number of the selected output points, and $\mathbf{L} \in \mathbb{R}^{q \times n}$ is the state-to-output matrix that maps the internal states to the output points.

Then, the objective of MOR is to produce a system of the lower order of the Eq. 2.6, that calculates the stress, as follows:

$$\tilde{\mathbf{C}}\dot{\tilde{\sigma}}(t) = \tilde{\mathbf{A}}\tilde{\sigma}(t) + \tilde{\mathbf{B}}\mathbf{j}(t), \quad \mathbf{y}(t) = \tilde{\mathbf{L}}\,\tilde{\sigma}(t) \tag{4.3}$$

where $\tilde{\mathbf{A}} \in \mathbb{R}^{r\times r}$, $\tilde{\mathbf{B}} \in \mathbb{R}^{r\times p}$ and $\tilde{\mathbf{L}} \in \mathbb{R}^{q\times r}$, with r being the reduced-order of the LTI ODE system.

The final reduced matrices are generated by firstly applying the EKS MM method already introduced in Section 4.4 to Eq. 2.6 and, ultimately, calculated as:

$$\tilde{\mathbf{C}} = \mathbf{V}^T\mathbf{E}\mathbf{V}, \quad \tilde{\mathbf{A}} = \mathbf{V}^T\mathbf{A}\mathbf{V}, \quad \tilde{\mathbf{B}} = \mathbf{V}^T\mathbf{B}, \quad \tilde{\mathbf{L}} = \mathbf{L}\mathbf{V} \tag{4.4}$$

With the formation of the needed matrices completed, we have reduced the original system to a sufficiently less expensive one. The new system needs fewer memory resources and less time to perform the EM analysis. This step is necessary, especially for the reduction of the total simulation time needed, since a clock tree network specifically has thousands and tens of thousands of discretization points, depending on the size of the original design it was extracted from [81]. The next step in our method is to simulate the reduced order model using the Backward-Euler (BE) differential approximation formula and solve the linear systems at each time step to calculate the stress values at every via and junction. For this step, the stress corresponds to the TTF defined in the original design's specifications.

Algorithm 3 Optimal EM-based Trojan Placement Procedure

1: Extract the clock tree network from the design.
2: Construct the corresponding discretized system from Korhonen's Eq. 2.1 and the generalised final Eq. 2.6 by finding the vias/junctions.
3: Do an EM analysis on the clock tree applying the MM method to obtain the reduced system 4.3.
4: Perform transient analysis based on the design lifetime on the output portion of vector σ.
5: Determine the percentage increase in the currents required to attain a desired TTF.
6: Pick the lower percentage as the point of attack to connect the stressing source of the EM-based HT.

The placement of the EM-based HT results in shortening the TTF to the attack's desired one. For this purpose, the following step in our methodology is to calculate the needed percentile increase of the current density. One essential aspect of the EM-based HT is to

remain stealthy, by masking its impact on the overall power consumption behind the natural process variations occurring in the die. With that in mind, the final step of our algorithm is to pick the point of attack that requires the minimum increase in current for the EM-based HT to be placed. The final design of the clock tree after the insertion can be seen in Fig. 4.2 and a summary of our methodology is found in Alg.3.

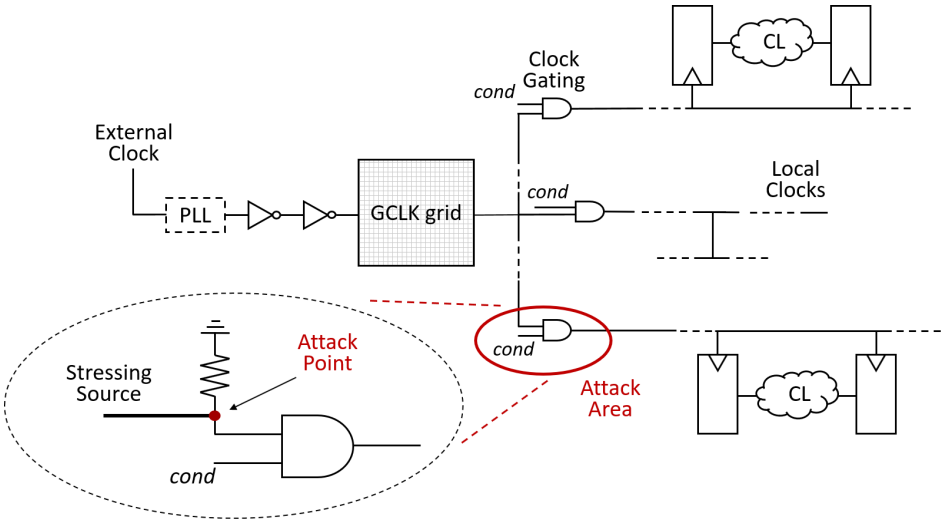


Figure 4.2: Instance of an EM-based HT inserted on the clock tree network. [1]

A byproduct of our methodology is the validation of the clock tree under attack as EM-safe. As part of deciding the insertion point for the HT, it exhaustively simulates the most vulnerable points to the creation of EM hotspots. Thus, if the introduced stress to all vias and junctions exceeds the process variation limits, the clock network can be considered EM-safe.

4.6 Evaluation of the methodology

4.6.1 Experimental setup

The proposed methodology was evaluated on three differently sized clock tree networks extracted from a set of microprocessor designs with random control logic and datapath. The benchmarks were synthesized using the Nangate 45nm PDK cell library and their TTF was specified to be 10 years, a usually targeted lifetime for microprocessors. The interconnects were modeled from the Cu DD technology and their critical stress for a void to be created was set at 100MPa [82]. Both the MM and the transient analysis parts of our methodology

for the experiments were implemented in MATLAB R2021 on a Windows computer having 32GB RAM and a 3.6 GHz Intel Core i7 CPU.

Table 4.3: Characteristics of the benchmarks

Benchmark	**#segments**	**#vias/junctions**	**#discr. points**	**TTF (y)**
clock tree 1	800	801	4018	10
clock tree 2	1000	1001	4557	10
clock tree 3	1200	1201	5438	10

The netlists are extracted and Eq.2.6 is formed. Table 4.3 provides the state of each benchmark right before our improved EM analysis is applied. Column *#segments* refers to the total number of the segments for each benchmark, while column *#vias/junctions* refers to the existing vias and junctions in the clock tree nets. The *#discr. points* column demonstrates the total number of the discretization points for the construction of the model and, last but not least, *TTF (y)* states the expected lifetime of the design as defined in the specifications and the benchmarks have achieved.

4.6.2 Assessment of the experimental results

We employed our methodology on the aforementioned benchmarks in order to find the optimal placement of the Trojan on the gated clock tree nets to reduce its TTF to 70% and 80% (7 and 8 years respectively). The EM-based HT placement results of the experiments are documented in the columns of Table 4.4. Column *#vias/junctions* is re-shown as a reference point for comparison since *#susceptible vias/junctions* reports the number of them that are closer to the critical stress and thus a favorable placement point for a stealthy insertion of the trojan. columns *Current increase percentage for 70% of TTF*, *Current increase percentage for 80% of TTF* demonstrates the minimum needed increase in the current density for the attack point to exceed the critical stress. Lastly, *simulation time (m)* reports the execution time of the proposed methodology.

Table 4.4: Experimental results of the methodology on clock trees

Benchmark	**#vias/junctions**	**#susceptible vias/junctions**	**Current increase percentage for 70% of TTF**	**Current increase percentage for 80% of TTF**	**simulation time (m)**
clock tree 1	801	47	8%	0.5%	1.162
clock tree 2	1001	104	5%	1%	1.490
clock tree 3	1201	79	7%	1.5%	2.328

Our method identified several susceptible points for the placement of the reliability-based HT on the extracted gated clock networks, as shown above. Furthermore, for both reducing the TTF at 70% and 80%, experimental results illustrate that the current increment needed for the attack is below 8% which poses a huge challenge for any detection technique utilizing side-channel analysis [27, 83]. Especially for the 80% of TTF the current increment can be considered totally insignificant. Additionally, it can be observed that simulating the EM stress for placing the EM-based HT is remarkably fast since we utilize a MM technique for obtaining the stresses only in vias and junctions.

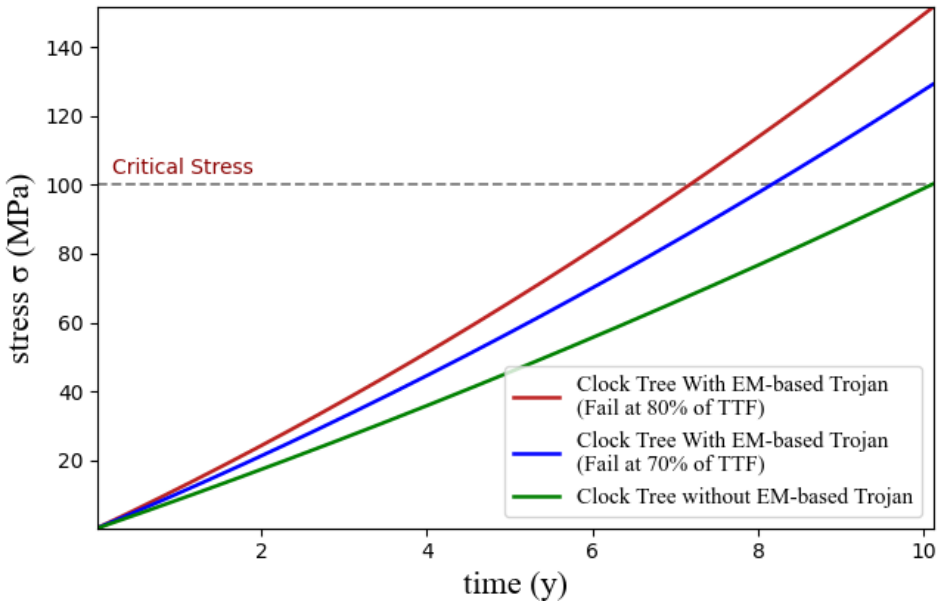


Figure 4.3: Transient simulation of the point of attack for *Clock Tree 3*.

Finally, Fig. 4.3 depicts the simulated waveforms of the EM stress of the reduced-order model at the attack point of the *Clock Tree 3* benchmark with and without the presence of the EM-based HT using a BE integration formula. As can be seen the injection of the Trojan can shorten the TTF making the clock tree network surpass the critical stress earlier.

Chapter 5

Sensitivity-aware Hardware Trojan Injection for SET Propagation and Soft Error Attacks

5.1 Introduction

The ongoing trend of technological miniaturization is, despite its intentions, increasingly intensifying the reliability concerns [84]. Radiation-induced transient faults pose a significant threat to the reliability of semiconductor chips. The primary sources of such faults include alpha particles released from the radioactive decay of the IC packaging materials, as well as high-energy particles, especially neutrons, originating from cosmic radiation entering the terrestrial atmosphere [85]. The problem occurs when particles like these strike a sensitive transistor, thus, generating numerous electron and hole pairs in it that are absorbed by the transistor's depletion region, and potentially causing a temporary glitch at the output of the respective logic gate [30]. This phenomenon is referred to as a Single Event Transient (SET). Although SETs are non-destructive and do not permanently damage the circuit, they may propagate through the combinational logic and be captured by a memory element creating a soft error.

Attackers increasingly exploit reliability issues, like radiation-induced transient faults, to cause malfunctions and disrupt the IC's proper behavior. This is achieved by injecting stealthy reliability-based Hardware Trojans (HTs) in key components in the IC. Reliability HTs with a trigger are activated by rare conditions, while remaining inactive, otherwise, rendering their

detection extremely challenging. Specifically, a SET-based HT [36] would remain passive until high-energetic particles trigger it. The most established ways to detect any HTs use methods that analyze the side-channel parameters. These methods rely on identifying any deviation from the design's specifications that would indicate the presence of an HT and are evaluated on benchmarks with one already inserted.

Inducing a soft error deliberately on a critical memory element can significantly disrupt the IC's functionality. However, not all disturbances, caused by various factors such as particle hits, necessarily result in a soft error. This is because they might not propagate through the circuit due to several factors, including the masking effects which offer a form of protection to the circuit functionality, and the specific characteristics of the SETs, i.e. their pulse width and height. Furthermore, the IC designer can identify any sensitive gates performing a Soft Error Rate (SER) analysis [44] and, thus, taking radiation-hardening measures. Therefore, the placement of a reliability-based HT aiming to exploit a SET that can create a soft error should be seriously considered. Besides, hardware trojan attacks based on and exploiting radiation effects on ICs are a subject that still has not been explored adequately.

In this paper, a method for creating designs injected with a SET-triggered reliability HT is introduced to provide challenging benchmarks for soft error attack identification techniques. The reliability HT is placed on the output of the target gate to broaden its SET pulse and ensure the creation of a soft error. SET characterization for each gate in the design and overall SER analysis is used to identify the sensitive target gates of the design for the injection. Another essential condition to be fulfilled is the stealthiness of the HT. For this reason, the potential target gates are filtered, excluding the ones being part of the critical path, as well as the prime candidates for radiation-hardening, since these would be obvious targets for an HT attack. We evaluate our method on various ISCAS '89 benchmarks by identifying the increase of targeted gates' sensitivity that follows the HT injection, and demonstrating to what extent SER is affected.

5.2 Single Event Transient pulses and soft errors

As the CMOS technology downscales, modern ICs have become significantly susceptible to various phenomena, including transient faults. A SET is a temporary disturbance in the electrical behavior of a gate caused by a particle hit. Such particles originate from various

sources, such as alpha particles emitted from the radioactive decay of IC packaging materials and high-energy particles from cosmic radiation. If a glitch occurs, it can propagate throughout the circuit and may be latched by at least one memory element, potentially leading to a soft error.

However, the emergence of a soft error can be prevented due to the existence of the three mechanisms, that is, Logical, Electrical, and Timing masking, as shown in Fig. 5.1. More specifically, Logical masking occurs when the arriving SET at a gate is blocked due to a controlling logic value of another input (a). Electrical masking is related to the SET shape modification during propagation and occurs when the SET is eliminated (b). Finally, Timing masking occurs when the SET arrives outside the latching window at a flip-flop input, thus not being able to be latched (c). A SER evaluation tool that assesses the IC sensitivity to radiation-induced faults should integrate both SET generation and masking mechanisms occurring at propagation. Such a tool can be utilized to analyze a design's susceptibility to SETs for exposing any potential hardware security vulnerabilities.

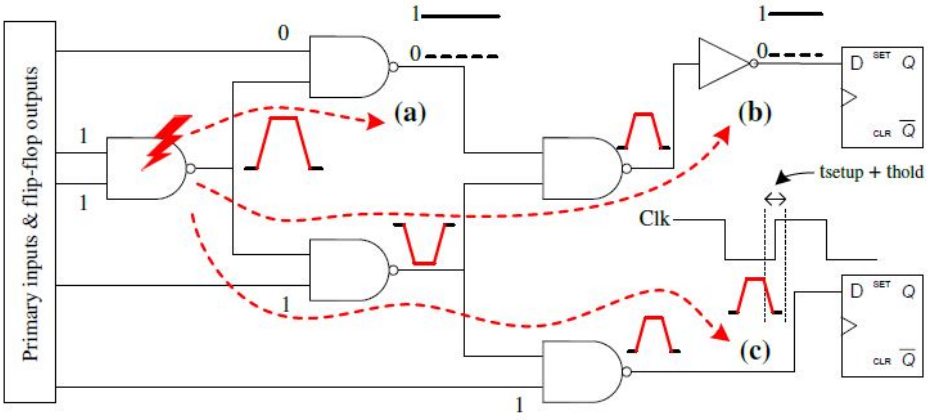
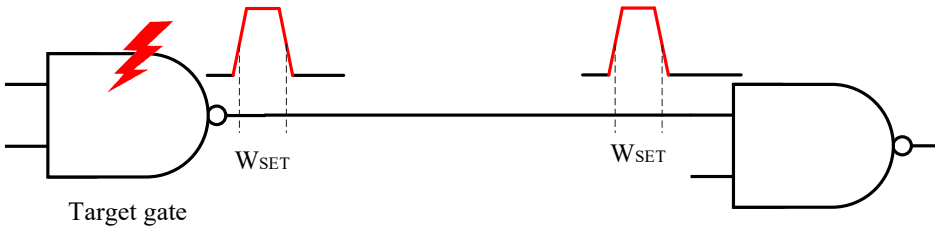


Figure 5.1: Average targeted gates sensitivity before and after the HT injection.

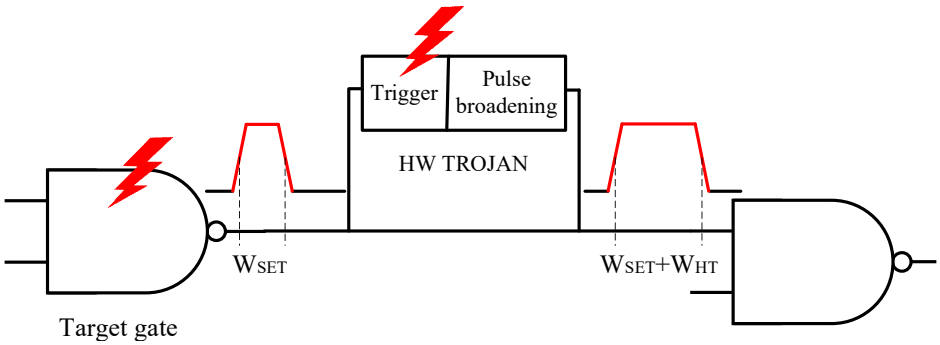
As mentioned before, due to the downscale of the technology, a key point in the emergence of soft errors is the generated SET width. This pulse depends, mainly, on the technology characteristics, as well as the source of radiation that affects the circuit. While logical and electrical masking's contribution to SER may not deviate significantly across technologies, timing masking is still crucial, given the trend of SET width to increase with technology downscaling [86,87]. The fact that the generated SET by itself may not always be sufficient, as regards its width, to be latched and become a soft error, is the motivation behind the proposed method of this work.

5.3 Single Event Transient based Hardware Trojan

In general, reliability Trojans cause long-term faults and disrupt the proper operation of the design by exploiting reliability phenomena and issues [49, 88]. Specifically, a reliability HT exploiting an occurring SET to attack memory elements of the design guarantees that the SET propagates from the targeted sensitive gate through the circuit and generates a soft error. This insurance is an essential element of the attack since, as mentioned before, not every SET propagates by default through the design to lead to a soft error. One way to increase the probability of propagation is by SET broadening, which can be applied by the reliability Trojan. The HT is inserted in the design so it interjects the output of a targeted gate, and as a result, when a radiation-induced transient fault is generated, it also passes through the HT. The output signal of the reliability HT that is broadened enough to successfully realize the intended attack is returned to the original path. As demonstrated in Fig. 5.2, the output payload, meaning the effect of the HT on the circuit, is the pulse broadened, which is re-converged to the original path.



(α′) Original path.



(β′) Hardware Trojan injected path.

Figure 5.2: The original design's path (a) and a SET-based HT bypassing it (b).

A circuitry that can be used for the design of a Trojan with such functionality was designed by the authors in [89]. The presented circuit can tune the pulse width resulting in a minimum pulse width of 80 ps and a maximum of 270 ns at its output. Thus, an HT can be designed

to generate a signal that respects the timing constraints of the IC's specifications, and it can propagate throughout the IC.

However, a Trojan only consisting of the above circuitry, would be always operating and broadening every output signal of the targeted gate and, as a consequence be more observable. This goes against one of the main characteristics of HTs, being stealthy. So, to mitigate this and further reinforce the HT stealthiness, a trigger based on SETs is introduced. In [36], the authors have explored SET-triggered HTs and have presented a design that follows that behavior. As a result, the HT is activated only under the condition of a SET occurring and, thus, is more challenging to be detected by any side-channel analysis techniques.

5.4 Proposed Algorithm

In this section, we present the sensitivity-aware HT injection methodology, primarily utilizing the evaluation of the gate vulnerability for the whole design to faults caused by radiation. The importance of this sensitivity analysis lies in identifying gates that are highly likely to result in soft errors, contributing to determining the optimal regions for attackers to insert a SET-based HT.

A modified version of the SER evaluation presented in [90] is utilized in this methodology, with the exception that it neglects Single Event Multiple Transients (SEMTs) as the proposed method targets each gate separately to identify its sensitivity. This study adopts the approach of [44] incorporating Dynamic Timing Analysis (DTA) for SET propagation, resulting in a more accurate SER analysis. A gate is considered sensitive when there is a high probability that a generated SET will propagate through the circuit and approach a memory element. In particular, the characterization of gate sensitivity focuses on each gate individually, injecting a specific number of particle strikes. In other words, as outlined in the Algorithm 4, a sufficient number of simulations are performed applying transient faults with different amplitudes on each gate and at various times within the clock period. In that regard, the resultant pulse is affected by the three masking mechanisms while propagating through the circuit. Ultimately, the sensitivity of gates corresponds to the probability that all these faults are captured by at least one memory element.

The significant number of simulations, involving various primary input vectors, and the circuit complexity, especially in the large-scale ones, are the main critical factors that render

this process quite time-consuming. However, it provides an accurate analysis to estimate the sensitivity of the gates contributing significantly to the ultimate objective of increasing the circuit's overall susceptibility and, thus, ensuring that more soft errors occur on the memory elements of the design. This outcome will be achieved by injecting the SET-based HT in less vulnerable gates, thereby increasing the probability that they may lead to a soft error. In particular, according to the algorithm, gates are sorted based on the probability that corresponds to their sensitivity levels. The gates chosen for the insertion of the HTs are those appertaining to a moderate susceptibility range, specifically, the gates that belong to levels ranging from 50% to 70% of the maximum evaluated sensitivity. The selection of this range stems from the principle that designers focus on enhancing the radiation-hardness of the critical gates. Therefore, the potential insertion of the reliability HTs in less susceptible gates will result in a significant increase in sensitivity.

Algorithm 4 Sensitivity-aware injection methodology of a SET-based HT.

1: Acquire design's netlist.
2: Perform multiple simulations to evaluate the sensitivity of every gate as well as the design's sensitivity as a whole.
3: Sort the gates based on their sensitivity levels.
4: Choose the potential target gates with an average susceptibility range from 50% to 70%.
5: Extract from the selected gates the ones belonging to the critical timing paths.
6: Pick up to 10% to become targeted gates and be injected with the SET-based HT.

Finally, the SET-based HT is important to remain stealthy. For this reason, the target gates that belong to the critical timing path are excluded from this procedure to ensure that the design's timing constraints are not violated. Furthermore, to ensure that any noticeable gate overhead is not observed, we select only up to 10% of the potential target gates. These, together with the fact that the targeted gates chosen are within the moderate susceptibility range already set, provide significantly more challenging benchmarks for any side-channel analysis identification method.

5.5 Evaluation of the methodology

5.5.1 Experimental setup

All the experiments are conducted on a Linux workstation with an 8-core Intel Xeon @3.5 GHz and 16 GB of memory. To obtain a reliable evaluation of our approach, several typical benchmarks from ISCAS ’89 suite are used. All the benchmarks are synthesized with Synopsys Design Compiler using the 45 nm Nangate OpenCell Library and the PnR is performed with Cadence Innovus.

Table 5.1: Characteristics of the benchmarks

Bench.	s344	s400	s449	s713	s1423	s5378	s9234	s13207
#Gates	231	200	270	504	991	3018	6983	9577
#FFs	15	21	19	19	74	179	228	669

The selection of the benchmarks is based on the following criteria; first, the number of logic gates should be sufficient enough to have an adequate number of sensitive gates as targets, and second, the circuit size should be large enough to sufficiently simulate SET propagation on long paths to obtain reliable results, while ensuring that the reliability HT will remain stealthy. Both of these criteria are met by the benchmarks chosen as Table 5.1 reports their characteristics, namely the total number of gates and flip-flops each benchmark contains.

5.5.2 Assessment of the experimental results

Table 5.2 presents the evaluation results for some benchmarks. More specifically, we demonstrate the percentage of the sensitive gates selected for the HT injection, presented in column *Targeted gates (%)*, after the appliance of the Algo. 4. The total number of gates is also re-shown for quick reference. The simulation results after the HT injection provide the average aggravation in sensitivity for the targeted gates, alongside the average increase in the SER for each benchmark. It is notable to comment that in the s9234 benchmark where more gates are targeted than the s5378, the sensitivity aggravation was greater in the latter. This is evidence that simply targeting more gates does not result in a more successful attack.

Table 5.2: Targeted gates sensitivity and SER variation results after the HT Injection

Bench.	# Gates	Targeted gates (%)	Change (%)	
			Sensitivity	SER
s344	231	8.6	+40.1	+5.87
s400	200	8.1	+39.4	+5.42
s449	270	7.9	+38.7	+5.24
s713	504	8.5	+37.6	+4.97
s1423	991	7.1	+34.1	+3.63
s5378	3018	6.2	+28.3	+3.22
s9234	6983	7.5	+23.7	+2.78
s13207	9577	6.9	+19.6	+2.49

A particle strike on a SET-based HT gate increases the probability of a soft error emergence. Therefore, it is crucial to highlight the attack's impact on the overall circuit sensitivity. In particular, we can observe that the percentage increase in SER is minimal, which is expected due to the limited number of target gates selected for injecting the SET-based HT compared to the total, as highlighted in Table 5.2. Choosing more than 10% of the overall IC's gates as targets endangers adding an observable gate overhead to the design and consequently make the SET-based HT vulnerable to any side-channel analysis detection techniques. Therefore, the circuits may indeed become a little more sensitive in their entirety, but their functionality is not visibly affected.

Our primary objective was to significantly aggravate the sensitivity of the chosen gates, and indeed an average increase of 32.6% is achieved. This fact is presented both by the percentage of the sensitivity in Table 5.2 and the average vulnerability of the target gates

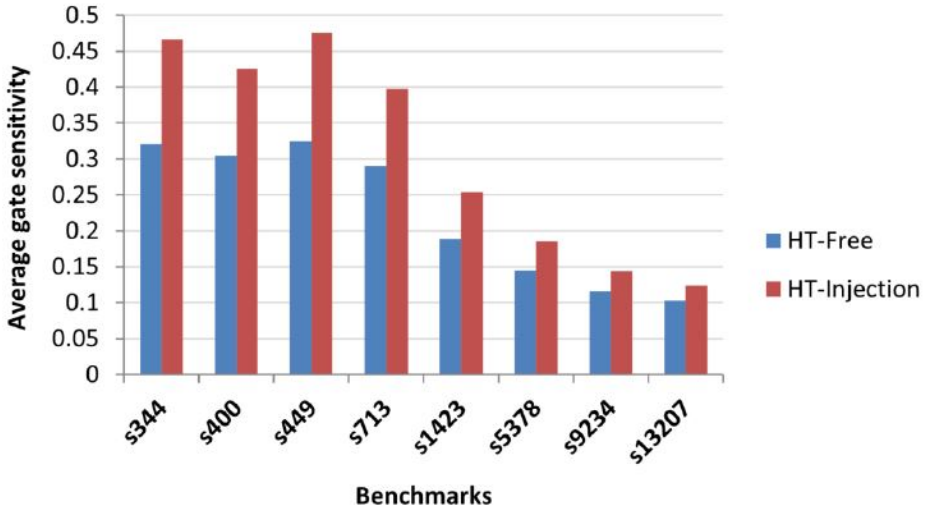


Figure 5.3: Average targeted gates sensitivity before and after the HT injection.

before and after the HT injection as illustrated in Fig. 5.3. Finally, the average difference in SER of the circuits between HT-free and HT-injected circuit versions is 4.2%.

Chapter 6

Conclusion

6.1 Summarising the thesis

Hardware security is a serious problem and a threat in the industry for over a decade. However, in recent years a new route has been discovered where HTs focus on exploiting reliability issues. These trojans aim at aggravating reliability phenomena like EM and SET faults. The former type of trojans, referred to as EM-based HTs, shortens the TTF of the attack point and therefore the lifetime of the whole design. An attacks especially on the clock tree network or the power grid affect the whole functionality of the chip by introducing only a small overhead and remain stealthy. The latter type of trojans. referred to as SET-based HTs, ensure the generation and propagation of a SET pulse in order to guarantee a soft error occurs, injecting a temporary fault in the chip's operations. The soft error would after some clock cycles correct itself erasing the traces of the payload of the HT and strengthening its stealthiness. In this research, three ways to create challenging benchmarks injected with reliability HTs were described. More specifically:

In Chapter 3, a security closure methodology for identifying potentially vulnerable lines in large-scale power grid structures was presented. The first step of the methodology is to identify the susceptible lines in the power grid that are most likely to fail, and then calculate the TTF with and without the presence of decap components. Experimental results demonstrate that our proposed methodology requires less than 33s for a line with as many as 597 segments to provide the analysis and the corresponding TTFs to the user, showcasing the achieved speed. Furthermore, the methodology exhibits high parallelizability, with the overall execution time primarily determined by the largest power grid line in the input.

In Chapter 4, an algorithm for the optimal placement of EM-based HTs on clock tree networks was presented. The methodology can efficiently create benchmarks with careful consideration of the stresses involved as well as the potential impact on circuit performance and power consumption, ensuring that the HTs remain stealthy from side-channel analysis techniques. The experimental results show that the suggested approach can create benchmarks that inject EM-based HTs with a current increase of less than 8% in less than 2.5 minutes.

In Chapter 5, a methodology for injecting a SET-based reliability HT is presented. The potential target gates was discovered by considering the sensitivity of the design's gates through a SER analysis, as well as excluding the more sensitive ones and from the remaining set, those that belong to critical timing paths. Thus, the proposed methodology ensures the stealthiness of the reliability HT and provides a challenging benchmark for evaluating any side-channel analysis identification techniques. The experimental results indicate an average increase of 32.6% in the sensitivity of the targeted gates and of 4.2% in SER.

In conclusion, the presented research work has provided three efficient, robust, and fast methodologies for creating challenging HT-inserted benchmarks. Acquiring and choosing infected benchmarks is a critical step in testing any HT detection techniques and adequately evaluating their efficiency and competence. For these reasons, these methodologies have been developed to further aid the efforts against hardware security attacks exploiting reliability issues.

6.2 Future work

In this thesis, three algorithms were developed for designing as well as implementing reliability-injected benchmarks. However, there is room for improvement in future research. Firstly, the work so far focuses only on some of the reliability issues, i.e. EM and SET faults. The research can be extended on the topics of Negative Bias Temperature Instability (NBTI), Gate Oxide short, and Mechanical Stress Effects. Secondly, these techniques utilize the naturally occurring process variations of the chip as a standard to decide the percentages of permitted added current. A more accurate calculation of the levels of process variations would result in choosing better-suited percentages, catered to each design rather than a blanket number.

Thirdly, all of these techniques, seen from an opposite point of view, can be detection

techniques for the reliability-based trojans they implement in theory. Properly and thoroughly evaluating their value as detection techniques can open new routes against the threat of HTs. Finally, if and when all these are achieved, they can be compiled into one software aiming to asses a design's vulnerability to any reliability-based HT in an efficient and in every respect.

Publications

[1] Alexandra Takou, Olympia Axelou, George Floros, Nestor Evmorfopoulos, and George Stamoulis. An optimal methodology for em-based hardware trojan placement on clock tree networks. In *2023 IEEE 66th International Midwest Symposium on Circuits and Systems (MWSCAS)*, pages 25–29, 2023.

[2] Alexandra Takou, Pavlos Stoikos, Moysis Moysis, George Floros, Nestor Evmorfopoulos, and George Stamoulis. An efficient security closure methodology for em-based attacks on power grid structures. In *2023 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, pages 1–4, 2023.

[3] Alexandra Takou, Georgios-Ioannis Paliaroutis, Pelopidas Tsoumanis, Nestor Evmorfopoulos, and George Stamoulis. Sensitivity-aware hardware trojan injection for set propagation and soft error attacks. In *2024 20th International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD)*, pages 1–4, 2024.

References

[1] Jens Lienig, Susann Rothe, Matthias Thiele, Nikhil Rangarajan, Mohammed Ashraf, Mohammed Nabeel, Hussam Amrouch, Ozgur Sinanoglu, and Johann Knechtel. Toward security closure in the face of reliability effects iccad special session paper. In *2021 IEEE/ACM International Conference On Computer Aided Design (ICCAD)*, pages 1–9, Nov 2021.

[2] Age Yeh. Trends in the global ic design service market. *DIGITIMES research*, 2012.

[3] Kan Xiao, Domenic Forte, Yier Jin, Ramesh Karri, Swarup Bhunia, and Mohammad Tehranipoor. Hardware trojans: Lessons learned after one decade of research. *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, 22(1):1–23, 2016.

[4] Ayush Jain and Ujjwal Guin. A novel tampering attack on aes cores with hardware trojans. In *2020 IEEE International Test Conference in Asia (ITC-Asia)*, pages 77–82. IEEE, 2020.

[5] Yu Liu, Yier Jin, Aria Nosratinia, and Yiorgos Makris. Silicon demonstration of hardware trojan design and detection in wireless cryptographic ics. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 25(4):1506–1519, 2016.

[6] R Naveenkumar, NM Sivamangai, A Napolean, and V Janani. A survey on recent detection methods of the hardware trojans. In *2021 3rd International Conference on Signal Processing and Communication (ICPSC)*, pages 139–143. IEEE, 2021.

[7] Mohammad Tehranipoor and Farinaz Koushanfar. A survey of hardware trojan taxonomy and detection. *IEEE Design & Test of Computers*, 27(1):10–25, 2010.

[8] Ujjwal Guin, Ziqi Zhou, and Adit Singh. Robust design-for-security architecture for enabling trust in ic manufacturing and test. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 26(5):818–830, 2018.

[9] Richard Wayne Jarvis and Michael G Mcintyre. Split manufacturing method for advanced semiconductor circuits, March 27 2007. US Patent 7,195,931.

[10] Kaushik Vaidyanathan, Renzhi Liu, Ekin Sumbul, Qiuling Zhu, Franz Franchetti, and Larry Pileggi. Efficient and secure intellectual property (ip) design with split fabrication. In *2014 IEEE international symposium on hardware-oriented security and trust (HOST)*, pages 13–18. IEEE, 2014.

[11] Farinaz Koushanfar, Inki Hong, and Miodrag Potkonjak. Behavioral synthesis techniques for intellectual property protection. *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, 10(3):523–545, 2005.

[12] Anirban Sengupta, Dipanjan Roy, and Saraju P. Mohanty. Triple-phase watermarking for reusable ip core protection during architecture synthesis. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 37(4):742–755, 2018.

[13] Jeyavijayan Rajendran, Youngok Pino, Ozgur Sinanoglu, and Ramesh Karri. Logic encryption: A fault analysis perspective. In *2012 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 953–958. IEEE, 2012.

[14] Rajat Subhra Chakraborty and Swarup Bhunia. Harpoon: An obfuscation-based soc design methodology for hardware protection. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 28(10):1493–1502, 2009.

[15] Jeyavijayan Rajendran, Vinayaka Jyothi, Ozgur Sinanoglu, and Ramesh Karri. Design and analysis of ring oscillator based design-for-trust technique. In *29th VLSI Test Symposium*, pages 105–110. IEEE, 2011.

[16] Yuan Cao, Chip-Hong Chang, and Shoushun Chen. A cluster-based distributed active current sensing circuit for hardware trojan detection. *IEEE Transactions on Information Forensics and Security*, 9(12):2220–2231, 2014.

[17] Hassan Salmani, Mohammad Tehranipoor, and Jim Plusquellic. A novel technique for improving hardware trojan detection and reducing trojan activation time. *IEEE transactions on very large scale integration (VLSI) systems*, 20(1):112–125, 2011.

[18] Giorgio Di Natale, Sophie Dupuis, and Bruno Rouzeyre. Is side-channel analysis really reliable for detecting hardware trojans? In *DCIS'2012: XVII Conference on Design of Circuits and Integrated Systems*, pages 238–242. Citeseer, 2012.

[19] MA Nourian, Mahdi Fazeli, and David Hély. Hardware trojan detection using an advised genetic algorithm based logic testing. *Journal of Electronic Testing*, 34:461–470, 2018.

[20] Vidya Govindan and Rajat Subhra Chakraborty. Logic testing for hardware trojan detection. *The Hardware Trojan War: Attacks, Myths, and Defenses*, pages 149–182, 2018.

[21] Yuanwen Huang, Swarup Bhunia, and Prabhat Mishra. Mers: statistical test generation for side-channel analysis based trojan detection. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 130–141, 2016.

[22] Hassan Salmani and Mohammad Tehranipoor. Layout-aware switching activity localization to enhance hardware trojan detection. *IEEE Transactions on Information Forensics and Security*, 7(1):76–87, 2011.

[23] Gor Piliposyan, Saqib Khursheed, and Daniele Rossi. Hardware trojan detection on a pcb through differential power monitoring. *IEEE Transactions on Emerging Topics in Computing*, 10(2):740–751, 2022.

[24] Mainak Banga and Michael S. Hsiao. Vitamin: Voltage inversion technique to ascertain malicious insertions in ics. In *2009 IEEE International Workshop on Hardware-Oriented Security and Trust*, pages 104–107, 2009.

[25] Devendra Rai and John Lach. Performance of delay-based trojan detection techniques under parameter variations. In *2009 IEEE International Workshop on Hardware-Oriented Security and Trust*, pages 58–65, 2009.

[26] Yiming Wen and Weize Yu. Combining thermal maps with inception neural networks for hardware trojan detection. *IEEE Embedded Systems Letters*, 13(2):45–48, 2020.

[27] Yier Jin and Yiorgos Makris. Hardware trojan detection using path delay fingerprint. In *2008 IEEE International Workshop on Hardware-Oriented Security and Trust*, pages 51–57, 2008.

[28] Sheng Wei and Miodrag Potkonjak. Scalable hardware trojan diagnosis. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 20(6):1049–1057, 2012.

[29] Aswin Sreedhar, Sandip Kundu, and Israel Koren. On reliability trojan injection and detection. *Journal of Low Power Electronics*, 8(5):674–683, 2012.

[30] R. C. Baumann. Radiation-induced soft errors in advanced semiconductor technologies. *IEEE Transactions on Device and materials reliability*, 5(3):305–316, 2005.

[31] George A. Sullivan. Search for reversal in copper electromigration. *Journal of Physics and Chemistry of Solids*, 28(2):347–350, 1967.

[32] Timothy C May and Murray H Woods. Alpha-particle-induced soft errors in dynamic memories. *IEEE transactions on Electron devices*, 26(1):2–9, 1979.

[33] J. F. Ziegler. Terrestrial cosmic rays. *IBM Journal of Research and Development*, 40(1):19–39, 1996.

[34] Hideyuki Nakamura, Taiki Uemura, Kan Takeuchi, Toshikazu Fukuda, Shigetaka Kumashiro, and Tohru Mogami. Scaling effect and circuit type dependence of neutron induced single event transient. In *2012 IEEE International Reliability Physics Symposium (IRPS)*, pages 3C–3. IEEE, 2012.

[35] Adrian Evans, Maximilien Glorieux, Dan Alexandrescu, Cesar Boatella Polo, and Véronique Ferlet-Cavrois. Single event multiple transient (semt) measurements in 65 nm bulk technology. In *2016 16th European Conference on Radiation and Its Effects on Components and Systems (RADECS)*, pages 1–6. IEEE, 2016.

[36] Paul A. Quintana; John McCollum; William A. Hill. Single event effect hardware trojans with remote activation. Technical Report AD1041451, Microsemi Corporation, San Jose California 95134, 2017.

[37] M. A. Korhonen, P. Bo/rgesen, K. N. Tu, and Che□Yu Li. Stress evolution due to electromigration in confined metal lines. *Journal of Applied Physics*, 73(8):3790–3799, 1993.

[38] Olympia Axelou, George Floros, Nestor Evmorfopoulos, and George Stamoulis. Fast electromigration stress analysis using low-rank balanced truncation for general interconnect and power grid structures. *Integration*, 89:197–206, 2023.

[39] Mohammad Abdullah Al Shohel, Vidya A. Chhabria, Nestor Evmorfopoulos, and Sachin S. Sapatnekar. Analytical modeling of transient electromigration stress based on boundary reflections. In *Procs. of the IEEE/ACM International Conference On Computer Aided Design*, pages 1–8, 2021.

[40] Olympia Axelou, Nestor Evmorfopoulos, George Floros, George Stamoulis, and Sachin S. Sapatnekar. A novel semi-analytical approach for fast electromigration stress analysis in multi-segment interconnects. In *2022 IEEE/ACM International Conference On Computer Aided Design (ICCAD)*, pages 1–7, 2022.

[41] Timothy C May and Murray H Woods. Alpha-particle-induced soft errors in dynamic memories. *IEEE transactions on Electron devices*, 26(1):2–9, 1979.

[42] James F Ziegler. Terrestrial cosmic rays. *IBM journal of research and development*, 40(1):19–39, 1996.

[43] Chong Leong Gan and Mohamad Zainudeen Moideen. Soft error mechanisms, modeling and mitigation. springer (2016). *Microelectronics reliability*, (74):81–81, 2017.

[44] Georgios Ioannis Paliaroutis, Pelopidas Tsoumanis, Nestor Evmorfopoulos, George Dimitriou, and Georgios I. Stamoulis. Set pulse characterization and ser estimation in combinational logic with placement and multiple transient faults considerations. *Technologies*, 8(1), 2020.

[45] GR Srinivasan, PC Murley, and HK Tang. Accurate, predictive modeling of soft error rate due to cosmic rays and chip alpha radiation. In *Proceedings of 1994 IEEE International Reliability Physics Symposium*, pages 12–16. IEEE, 1994.

[46] Riaz Naseer, Jeff Draper, Younes Boulghassoul, Sandeepan DasGupta, and Art Witulski. Critical charge and set pulse widths for combinational logic in commercial 90nm cmos technology. In *Proceedings of the 17th ACM Great Lakes symposium on VLSI*, pages 227–230, 2007.

[47] Fan Wang and Vishwani D Agrawal. Soft error rate determination for nanoscale sequential logic. In *2010 11th International Symposium on Quality Electronic Design (ISQED)*, pages 225–230. IEEE, 2010.

[48] C.-C. Yang et al. Microstructure modulation for resistance reduction in copper interconnects. In *Proceedings of the IEEE International Interconnect Technology Conference (IITC)*, pages 1–3, 2017.

[49] Chase Cook, Sheriff Sadiqbatcha, Zeyu Sun, and Sheldon X.-D. Tan. Reliability based hardware trojan design using physics-based electromigration models. *Integration*, 66:9–15, 2019.

[50] Xiaoxiao Wang, Hassan Salmani, Mohammad Tehranipoor, and Jim Plusquellic. Hardware trojan detection and isolation using current integration and localized current analysis. In *2008 IEEE International Symposium on Defect and Fault Tolerance of VLSI Systems*, pages 87–95, 2008.

[51] J.N. Kozhaya, S.R. Nassif, and F.N. Najm. A multigrid-like technique for power grid analysis. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 21(10):1148–1160, 2002.

[52] Shiyou Zhao, Kaushik Roy, and Cheng-Kok Koh. Decoupling capacitance allocation and its application to power-supply noise-aware floorplanning. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 21(1):81–92, 2002.

[53] Stefano Piersanti, Francesco de Paulis, Carlo Olivieri, and Antonio Orlandi. Decoupling capacitors placement for a multichip pdn by a nature-inspired algorithm. *IEEE Transactions on Electromagnetic Compatibility*, 60:1678–1685, 2018.

[54] Logan Horowitz and Robert Carl Nikolai Pilawa-Podgurski. On decoupling capacitor size in gan-based power converters. *2022 IEEE 23rd Workshop on Control and Modeling for Power Electronics (COMPEL)*, pages 1–5, 2022.

[55] Yuuta Satomi, Koutaro Hachiya, Toshiki Kanamoto, and Atsushi Kurokawa. Optimization of full-chip power distribution networks in 3d ics. *2018 IEEE 3rd International Conference on Integrated Circuits and Microsystems (ICICM)*, pages 134–138, 2018.

[56] Pavlos Stoikos, George Floros, Dimitrios Garyfallou, Nestor Evmorfopoulos, and George Stamoulis. A fast semi-analytical approach for transient electromigration analysis of interconnect trees using matrix exponential. In *Proceedings of the 28th Asia and South Pacific Design Automation Conference*, ASPDAC '23, page 1–6, 2023.

[57] Haifeng Qian and Sachin S. Sapatnekar. Fast poisson solvers for thermal analysis. In *2010 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pages 698–702, 2010.

[58] Jithendra Srinivas, Madhusudan Rao, Sukumar Jairam, H Udayakumar, and Jagdish Rao. Clock gating effectiveness metrics: Applications to power optimization. In *2009 10th International Symposium on Quality Electronic Design*, pages 482–487. IEEE, 2009.

[59] Monica Donno, Enrico Macii, and Luca Mazzoni. Power-aware clock tree planning. In *Proceedings of the 2004 international symposium on Physical design*, pages 138–147, 2004.

[60] Te-Jui Wang, Shih-Hsu Huang, Wei-Kai Cheng, and Yih-Chih Chou. Top-level activity-driven clock tree synthesis with clock skew variation considered. *2016 IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 2591–2594, 2016.

[61] Monica Donno, Enrico Macii, and Luca Mazzoni. Power-aware clock tree planning. In *Proceedings of the 2004 International Symposium on Physical Design*, ISPD '04, page 138–147, New York, NY, USA, 2004. Association for Computing Machinery.

[62] Jitesh Shinde and SS Salankar. Clock gating—a power optimizing technique for vlsi circuits. In *2011 annual IEEE India conference*, pages 1–4. IEEE, 2011.

[63] G. De Luca, G. Antonini, and P. Benner. A parallel, adaptive multi-point model order reduction algorithm. In *2013 IEEE 22nd Conference on Electrical Performance of Electronic Packaging and Systems*, pages 115–118, 2013.

[64] Tamara Bechtold. Model order reduction of electro-thermal mems [elektronische ressource] /. 01 2005.

[65] Chrysostomos Chatzigeorgiou, Dimitrios Garyfallou, George Floros, Nestor Evmorfopoulos, and George Stamoulis. Exploiting extended krylov subspace for the reduction of regular and singular circuit models. pages 773–778, 01 2021.

[66] B. Besselink, U. Tabak, A. Lutowska, N. van de Wouw, H. Nijmeijer, D.J. Rixen, M.E. Hochstenbach, and W.H.A. Schilders. A comparison of model reduction techniques from structural dynamics, numerical mathematics and systems and control. *Journal of Sound and Vibration*, 332(19):4403–4422, 2013.

[67] George Floros, Nestor Evmorfopoulos, and George Stamoulis. Efficient hotspot thermal simulation via low-rank model order reduction. In *2018 15th International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD)*, pages 205–208, 2018.

[68] Qingjian Yu and Ernest S Kuh. Exact moment matching model of transmission lines and application to interconnect delay estimation. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 3(2):311–322, 1995.

[69] Francesca Randone, Luca Bortolussi, Emilio Incerto, and Mirco Tribastone. Inference of probabilistic programs with moment-matching gaussian mixtures. *Proceedings of the ACM on Programming Languages*, 8:1882 – 1912, 2023.

[70] Dharma Pal Singh Chauhan. Model order reduction of continuous interval systems via time moment matching and pole clustering approaches. 2018.

[71] Luis G. Crespo, Sean P. Kenny, and Daniel P. Giesy. Moment-matching predictor models with a linear staircase structure. 2018.

[72] Maria Cruz Varona, Mikhail Pak, and Boris Lohmann. Towards output krylov subspace-based nonlinear moment matching. 2019.

[73] Pavlos Stoikos, Dimitrios Garyfallou, George Floros, Nestoras E. Evmorfopoulos, and George I. Stamoulis. The extended and asymmetric extended krylov subspace in moment-matching-based order reduction of large circuit models. *ArXiv*, abs/2204.02467, 2022.

[74] Mohsen Vakilzadeh, Mohammad Eghtesad, Ramin Vatankhah, and Masih Mahmoodi. A krylov subspace method based on multi-moment matching for model order reduction of large-scale second order bilinear systems. *Applied Mathematical Modelling*, 2018.

[75] Lennart Frie and Peter Eberhard. On shift selection for krylov subspace based model order reduction. *Multibody System Dynamics*, pages 1–21, 2023.

[76] A. Odabasioglu, M. Celik, and L.T. Pileggi. Prima: passive reduced-order interconnect macromodeling algorithm. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 17(8):645–654, 1998.

[77] Nicodemus Banagaaya, Giuseppe Alì, Wil Schilders, and Caren Tischendorf. Implicit index-aware model order reduction for rlc/rc networks. pages 1–6, 01 2014.

[78] Mohammad Abdullah Al Shohel, Vidya A. Chhabria, and Sachin S. Sapatnekar. A new, computationally efficient "blech criterion" for immortality in general interconnects. In *2021 58th ACM/IEEE Design Automation Conference (DAC)*, page 913–918. IEEE Press, 2021.

[79] Sandeep Chatterjee, Valeriy Sukharev, and Farid N. Najm. Fast physics-based electromigration assessment by efficient solution of linear time-invariant (lti) systems. In *2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pages 659–666, 2017.

[80] Olympia Axelou, George Floros, Nestor Evmorfopoulos, and George Stamoulis. Accelerating electromigration stress analysis using low-rank balanced truncation. In *2022 18th International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD)*, pages 1–4, 2022.

[81] Neeraja John. Clock tree synthesis based on wire length minimization algorithm. 2015.

[82] Mohammad Abdullah Al Shohel, Vidya A. Chhabria, Nestor Evmorfopoulos, and Sachin S. Sapatnekar. Analytical modeling of transient electromigration stress based on boundary reflections. In *2021 IEEE/ACM International Conference On Computer Aided Design (ICCAD)*, pages 1–8, 2021.

[83] Dakshi Agrawal, Selçuk Baktir, Deniz Karakoyunlu, Pankaj Rohatgi, and Berk Sunar. Trojan detection using ic fingerprinting. *2007 IEEE Symposium on Security and Privacy (SP '07)*, pages 296–310, 2007.

[84] Premkishore Shivakumar, Michael Kistler, Stephen W Keckler, Doug Burger, and Lorenzo Alvisi. Modeling the effect of technology trends on the soft error rate of combinational logic. In *Proceedings International Conference on Dependable Systems and Networks*, pages 389–398. IEEE, 2002.

[85] Robert C Baumann. Soft errors in advanced semiconductor devices-part i: the three radiation sources. *IEEE Transactions on device and materials reliability*, 1(1):17–22, 2001.

[86] Balaji Narasimham, Bharat L Bhuva, Ronald D Schrimpf, Lloyd W Massengill, Matthew J Gadlage, Oluwole A Amusan, William Timothy Holman, Arthur F Witulski, William H Robinson, Jeffrey D Black, et al. Characterization of digital single event transient pulse-widths in 130-nm and 90-nm cmos technologies. *IEEE Transactions on Nuclear Science*, 54(6):2506–2511, 2007.

[87] Anand Dixit and Alan Wood. The impact of new technology on soft error rates. In *2011 International Reliability Physics Symposium*, pages 5B–4. IEEE, 2011.

[88] Alexandra Takou, Olympia Axelou, George Floros, Nestor Evmorfopoulos, and George Stamoulis. An optimal methodology for em-based hardware trojan placement on clock tree networks. In *2023 IEEE 66th International Midwest Symposium on Circuits and Systems (MWSCAS)*, pages 25–29. IEEE, 2023.

[89] Shaoqiang Chen, Shengxi Diao, Pengtao Li, Takahiro Nakamura, Masahiro Yoshita, Guoen Weng, Xiaobo Hu, Yanling Shi, Yiqing Liu, and Hidefumi Akiyama. Broadband tunable integrated cmos pulser with 80-ps minimum pulse width for gain-switched semiconductor lasers. *Scientific reports*, 7(1):6878, 2017.

[90] Georgios-Ioannis Paliaroutis, Pelopidas Tsoumanis, Dimitrios Garyfallou, Anastasis Vagenas, Nestor Evmorfopoulos, and George Stamoulis. Accurate soft error rate evaluation using event-driven dynamic timing analysis. In *2023 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, pages 1–6, 2023.