

T.R.
GEBZE TECHNICAL UNIVERSITY
GRADUATE SCHOOL

**SECURITY-AWARE OPTIMIZATION OF ANALOG
INTEGRATED CIRCUITS**



ABDULLAH BAYRAM

A THESIS OF MASTER OF SCIENCE
DEPARTMENT OF ELECTRONICS ENGINEERING

ADVISOR: ASSOC. PROF. ENGIN AFACAN

OCTOBER 2025

T.R.
GEBZE TECHNICAL UNIVERSITY
GRADUATE SCHOOL

**SECURITY-AWARE OPTIMIZATION OF ANALOG
INTEGRATED CIRCUITS**



ABDULLAH BAYRAM

A THESIS OF MASTER OF SCIENCE
DEPARTMENT OF ELECTRONICS ENGINEERING

ADVISOR: ASSOC. PROF. ENGIN AFACAN
Co-ADVISOR: DR. HARALAMPOS STRATIGOPOULOS

OCTOBER 2025

T.C.
GEBZE TEKNİK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

**ANALOG TÜMLEŞİK DEVRELERDE GÜVENLİK-
DUYARLI OPTİMİZASYON**

ABDULLAH BAYRAM

YÜKSEK LİSANS TEZİ
ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI

DANIŞMAN: DOÇ. DR. ENGIN AFACAN
2. DANIŞMAN: DR. HARALAMPOS STRATIGOPOULOS

EKİM 2025



MASTER of SCIENCE JURY APPROVAL FORM

A thesis submitted by Abdullah, Bayram, defended on 10/10/2025 before the jury formed with the 30/06/2025 date and 2025/34 numbered decision of the GTU Graduate Administration Board, has been accepted as a MASTER of SCIENCE thesis in the Department of Electronics Engineering.

JURY

MEMBER

(THESIS ADVISOR) : Assoc. Prof. Engin Afacan

MEMBER : Assist. Prof. İhsan Çiçek

MEMBER : Assist. Prof. Okan Zafer Batur

APPROVAL

Gebze Technical University Graduate Administration Board
...../...../..... date and/..... numbered decision.

SIGNATURE/SEAL

ABSTRACT

As the digitalization of daily life increases, it causes a growing demand for electronic devices. Accelerating the design process of integrated circuits is essential to meeting the growing demand for rapid and efficient electronic system development. Inherent difficulties with IC (Integrated circuit) design makes meeting the demand more difficult especially on analog domain. Advancements in automation and novel fabrication methods have contributed to the emergence of fabless design, leading to enhanced accessibility and widespread adoption of integrated circuit (IC) development. However, with the acceleration of design processes and the growing digitalization of systems, malicious activities such as intellectual property (IP) theft have also increased. Furthermore, reverse engineering has become an increasingly frequent practice. Although the act is not inherently illegal, it can still result in significant violations of IP rights and contribute to the emergence of counterfeit ICs. Threats against IPs create major problems for IP holders, especially financial losses but are not limited to that. Counterfeit devices pose serious risks, including potential threats to consumer health, breaches of national security, and other significant consequences. Security-aware design remains a challenging task, often requiring substantial manual effort and specialized expertise. This challenge is particularly evident in the analog domain, where security considerations are still underdeveloped and remain in a relatively immature state. Significant advances have been made in the area of digital circuits in the effort to thwart IP piracy, to detect/prevent insertion of hardware Trojans and to protect against reverse engineering. However, analog design has not kept pace. Fundamental differences between digital and analog circuits make digital solutions less applicable in analog domain. Most of the digital devices depend on analog subblocks. Given that most of the counterfeit devices are analog based, securing analog design should be mandatory aspect for hardware security. The present study investigates common automation techniques, major security threats against ICs, and widely used defenses. This study also proposes a security automation approach that bridges analog design automation and hardware security, providing a foundational step toward enabling security automation in analog design. The proposed approach is then applied and assessed on key analog circuits to validate the method, though the approach is not limited to these specific circuits. The goal is to propose a strong security automation approach to mitigate reverse engineering and IC piracy. The utilized locking mechanisms help designers protect the rights of IP owners by obfuscating the sizes of transistors. Leveraging the power of automation, the implementation of locking mechanisms becomes more accessible and practical for circuit designers. To the best of our knowledge, this work presents the first implementation of security-aware optimization. This approach has the potential to enhance the security of analog circuits and protect intellectual property.

Keywords: Analog Integrated Circuits, Design Automation, IP Piracy, Hardware Security, Locking Methods, Reverse Engineering

ÖZET

Günlük hayattaki artan dijitalleşme elektronik cihazların talebinde önemli bir ölçüde artışa sebep olmuştur. Bu artışın karşılanması için tümleşik devre tasarımının hızlanması önemlidir. Tümleşik devre tasarımını doğası gereği olan zorlukları, özellikle analog temelli yapılar için bu talebin karşılanmasını bir hayli zorlaştırmaktadır. Otomasyonun ve yeni imalat teknikleri fabrikasız üretimin önünü açarak daha ulaşılabilir ve yaygın, tümleşik devre tasarımının önünü açmıştır. Ancak tasarım hızının ve dijitalleşmenin artması fikri mülkiyet hırsızlığı gibi kötü niyetli çalışmaları beraberinde getirmiştir. Bununla beraber tersine mühendislik oldukça yaygınlaşmıştır. Tersine mühendislik doğrudan yasadışı bir eylem olmasa da fikri mülkiyet haklarını ciddi şekilde ihlalin önünü açabilir ve sahte tümleşik devrelerin ortaya çıkmasına katkı sağlayabilir. Tümleşik devrelere yönelik bu tip tehditler fikri mülkiyet sahipleri için ekonomik kayıplarla sınırlı kalmaksızın ciddi problemler oluşturmaktadır. Örnek vermek gerekirse sahte cihazlar tüketiciler için sağlık riskleri oluşturabilir, milli güvenlikte zafiyetlere sebebiyet verebilir ve dahası. Güvenliğe duyarlı tasarım, genellikle önemli ölçüde elle çaba ve uzmanlık gerektiren zorlu bir görev olmaya devam etmektedir. Analog güvenliğin henüz yeterince olgunlaşmamış olması, söz konusu zorlukların analog devrelerde daha belirgin şekilde ortaya çıkmasına neden olmaktadır. Dijital devreler için fikri mülkiyet korsanlığını durdurmada, donanım Truva atlarını tespit etme/önlemede, tersine mühendisliğe karşı korumada ciddi adımlar atılmıştır ancak analog devreler için bu ilerleme yakalanılamamıştır. Dijital ve analog devreler arasındaki temel farklar dijital çözümlerin analog tarafında kullanılabilirliğini kısıtlamaktadır. Dijital cihazların çoğu analog alt-blokları temelinde barındırır. Sahte cihazların çoğunun analog tabanlı olduğu göz önüne alındığında, analog tasarımın güvenliğini sağlamak donanım güvenliği için elzemdir. Bu tezde, yaygın otomasyon tekniklerini, tümleşik devrelere yönelik başlıca güvenlik tehditlerini ve yaygın olarak kullanılan savunmaları incelemektedir. Bu çalışma aynı zamanda analog tasarım otomasyonu ve donanım güvenliği arasında köprü kurmakta ve güvenli analog devre otomasyonunu gerçekleştirilmesine yönelik temel bir adım sağlamaktadır. Daha sonra, önerilen yaklaşım seçilen devrelere özel olmamakla beraber önemli analog devreler üzerinde uygulanmış ve test edilmiştir. Amaç güçlü bir güvenlik otomasyonu ortaya koyup tersine mühendisliğin ve fikri mülkiyet korsanlığının önüne geçmektir. Kullanılan kilitleme yöntemi transistör boyutlarının gizlenmesi ile tasarımcıların fikri mülkiyet sahiplerinin haklarını korumasına yardımcı olur. Otomasyonun gücüyle bu kilitleme yönteminin uygulanması kolaylaşacak ve tasarımcılar için daha ulaşılabilir bir hale getirecektir. Bildiğimiz kadarıyla bu çalışma, güvenliğe duyarlı optimizasyonun ilk uygulamasını sunmaktadır. Bu şekilde analog devrelerin güvenliği güçlenecek ve fikri mülkiyetler korunabilecektir.

Anahtar Kelimeler: Analog Tümleşik Devreler, Devre Otomasyonu, Fikri Mülkiyet Korsanlığı, Donanım Güvenliği, Kilitleme

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my advisor, Engin Afacan, his continuous support, valuable guidance, and thoughtful feedback. I also extend my appreciation to my co-advisor, Haralampos Stratigopoulos, for his insightful contributions and technical guidance.

Special thanks to the members of my thesis defense committee, İhsan Çiçek and Okan Zafer Batur, for their time, valuable comments, and constructive suggestions, which have helped improve the quality of this work.

Thanks, should also go to my friends and colleagues, especially to members of LAMBDA, Enes Sağlıcan and Hakan Taşkiran, for their helpful discussions, encouragement, and companionship throughout this journey.

Finally, I wish to express my heartfelt appreciation to my wife, Rumeysa, and to my family for their love, patience, and support.

TABLE OF CONTENTS

ABSTRACT	v
ÖZET	vi
ACKNOWLEDGEMENTS	vii
TABLE OF CONTENTS	viii
LIST OF SYMBOLS AND ABBREVIATIONS	ix
LIST OF FIGURES	x
LIST OF TABLES	xii
1. INTRODUCTION	1
2. BACKGROUND	5
2.1 Analog IC Design Automation and Optimization	5
2.2 Hardware Security and Trust	8
2.2.1 Threats	9
2.2.2 Defenses	13
3. SECURITY AWARE OPTIMIZATION	22
3.1 Defense: Locking	23
3.2 Optimization: Particle Swarm Optimization	24
3.3 Attack model: Brute Force	25
4. PROPOSED APPROACH	26
5. CASE STUDIES	29
5.1 Two-stage amplifier	30
5.1.1 Optimization of Two-Stage Amplifier (without security)	30
5.1.2 Partial Optimization of Two-stage amplifier with 8-bit lock	32
5.1.3 Full Optimization of Two-stage amplifier with 8-bit lock	37
5.1.4 Summary of Two stage amplifier optimization	42
5.2 Bandgap Reference Circuit	43
5.2.1 Optimization of Bandgap Reference Circuit (without security)	43
5.2.2 Partial Optimization of Bandgap Reference with 8-bit lock	45
5.2.3 Full Optimization of BGR with 8-bit lock	49
5.2.4 Summary of Bandgap Reference Optimization	54
6. CONCLUSION AND FUTURE WORK	55
REFERENCES	57
BIOGRAPHY	63
PUBLICATIONS AND PRESENTATIONS FROM THE THESIS	64

LIST OF SYMBOLS AND ABBREVIATIONS

AV	: Gain
BGR	: Bandgap Reference Circuit
BW	: Bandwidth
CMOS	: Complementary Metal Oxide Semiconductor
DPA	: Differential Power Analysis
HT	: Hardware Trojan
IC	: Integrated Circuit
IP	: Intellectual Property
P	: Power
PKC	: Public Key Cryptography
PLL	: Phase Locked Loop
PM	: Phase Margin
POF	: Pareto-Optimal Fronts
PSO	: Particle Swarm Optimization
PTAT	: Proportional To Absolute Temperature
PUF	: Physical Unclonable Function
RF	: Radio Frequency
SoCs	: System-on-a-Chip
TC	: Temperature Coefficient

LIST OF FIGURES

	<u>Page</u>
Figure 1: IC product launch steps difference between fabless and conventional IC company.	2
Figure 2: A general flow of circuit design automation.	6
Figure 3: Pareto-optimal front for multi-objective optimization.	7
Figure 4: Threats through ICs lifetime.	8
Figure 5: IC piracy and overbuilding.	9
Figure 6: General scheme of a side-channel attack.	12
Figure 7: Transistors connected in series with varying V_t .	13
Figure 8: Fake contact example for transistors connected in parallel.	14
Figure 9: Example of split manufacturing scheme.	15
Figure 10: Size obfuscation with vector-based configuration.	17
Figure 11: Sizing obfuscation with mesh-based configuration.	19
Figure 12: Combinational locking implementation.	23
Figure 13: Particle swarm optimization.	24
Figure 14: Brute force attack for 6-bit lock.	25
Figure 15: Obfuscation of selected transistor.	26
Figure 16: Security aware optimization.	27
Figure 17: Flow of case studies.	29
Figure 18: Two-stage amplifier. Components shown in red are included in the optimization process.	30
Figure 19: Average performance cost of TSO amplifier.	31
Figure 20: Two-stage amplifier with 8-bit lock. Transistors shown in red are included in the optimization process.	32
Figure 21: Average Performance Cost of TSO Amplifier with 8-bit Lock (600 generation)	33
Figure 22: Average Performance Cost of TSO Amplifier with 8-bit Lock (1200 generation)	33
Figure 23: Error rates for each incorrect keys (56) satisfying the threshold after 600 and 1200 generations.	34
Figure 24: Average Performance + Security Cost of TSO Amplifier with 8-bit Lock (600 generation)	35
Figure 25: Average Performance + Security Cost of TSO Amplifier with 8-bit Lock (1200 generation)	35
Figure 26: Error rates for each incorrect keys (28) satisfying the threshold after 600 and 1200 generations.	36
Figure 27: Two-stage amplifier with 8-bit lock. Components shown in red are included in the optimization process.	37
Figure 28: Average Performance Cost of TSO Amplifier with 8-bit Lock (600 generations)	38
Figure 29: Average Performance Cost of TSO Amplifier with 8-bit Lock (1200 generations)	38

Figure 30: Error rates for each incorrect keys (17) satisfying the threshold after 600 generation.	39
Figure 31: Error rates for each incorrect keys (32) satisfying the threshold after 1200 generation.	39
Figure 32: Average Performance + Security Cost of TSO Amplifier with 8-bit Lock (600 generation)	40
Figure 33: Average Performance + Security Cost of TSO Amplifier with 8-bit Lock (1200 generation)	40
Figure 34: Error rates for each incorrect keys (1) satisfying the threshold after 1200 generation.	41
Figure 35: Error rates for each incorrect keys (0) satisfying the threshold after 1200 generation.	41
Figure 36: Bandgap Reference Circuit. Components shown in red are included in the optimization process.	43
Figure 37: Average Performance Cost of BGR.	44
Figure 38: Bandgap Reference Circuit with 8-bit lock. Components shown in red are included in the optimization process.	45
Figure 39: Average Performance Cost of BGR with 8-bit Lock (600 generation)	46
Figure 40: Average Performance Cost of BGR with 8-bit Lock (1200 generation)	46
Figure 41: Error rates for each incorrect keys (15) satisfying the threshold after 600 and 1200 generations.	47
Figure 42: Average Performance + Security Cost of BGR Amplifier with 8-bit Lock (600 generation)	48
Figure 43: Average Performance + Security Cost of BGR Amplifier with 8-bit Lock (1200 generation)	48
Figure 44: Error rates for each incorrect keys (0) satisfying the threshold after 600 and 1200 generation.	49
Figure 45: BGR with 8-bit lock. Components shown in red are included in the optimization process.	49
Figure 46: Average Performance Cost of BGR with 8-bit Lock (600 generation)	50
Figure 47: Average Performance Cost of BGR with 8-bit Lock (1200 generation)	50
Figure 48: Error rates for each incorrect keys (25) satisfying the threshold after 600 generation.	51
Figure 49: Error rates for each incorrect keys (31) satisfying the threshold after 1200 generation.	51
Figure 50: Average Performance + Security Cost of BGR with 8-bit Lock (600 generation)	52
Figure 51: Average Performance + Security Cost of BGR with 8-bit Lock (1200 generation)	52
Figure 52: Error rates for each incorrect keys (16) satisfying the threshold after 600 generation.	53
Figure 53: Error rates for each incorrect keys (0) satisfying the threshold after 1200 generation.	53

LIST OF TABLES

	<u>Page</u>
Table 1: Particle Swarm Parameters	25
Table 2: Optimization properties.	30
Table 3: Performance specifications of the best member after 600 generations of performance optimization.	32
Table 4: Performance specifications of the best member after 600 and 1200 generations of performance optimization.	33
Table 5: Performance specifications of the best member after 600 and 1200 generations of performance and security optimization.	35
Table 6: Performance specifications of the best member after 600 and 1200 generations of performance optimization.	38
Table 7: Performance specifications of the best member after 600 and 1200 generations of performance and security optimization.	40
Table 8: Summary of Security Results for Two Stage Amplifier.	42
Table 9: Performance specifications of the best member after 600 generations of performance optimization.	44
Table 10: Performance specifications of the best member after 600 and 1200 generations of performance optimization.	46
Table 11: Performance specifications of the best member after 600 and 1200 generations of performance and security optimization.	48
Table 12: Performance specifications of the best member after 600 and 1200 generations of performance optimization.	50
Table 13: Performance specifications of the best member after 600 and 1200 generations of performance and security optimization.	52
Table 14: Summary of Security Results for BGR.	54

1. INTRODUCTION

Demand on the electronical devices has increased dramatically in the last decades. Vast digitalization of the many systems leads to immense requirements on many different electronic devices. From kitchens to hospitals, farms to corporates, schools to government, electronic devices are used to improve efficiency, reduce costs, and bring better quality of life. Given the increasing integration of electronics into daily life, it is imperative for the design process to develop in order to address the growing complexity and performance expectations.

To meet this demand, many innovative design and production methods are developed. Previously developed optimization algorithms that were used to solve mathematical problems embodied into circuit design flow. This shift has led to significant advancements in both analog and digital design methodologies, introducing new perspectives on hardware development. Leveraging advances in automation and optimization, design automation has gained significant popularity within the industry. This approach allows design houses to accelerate the development of modern designs, enhancing both efficiency and productivity.

Manufacturing processes must keep pace with advancements in design flows to ensure seamless integration and maintain overall system efficiency. One of the most significant production models developed to address this growing need is the fabless design approach. In fabless production, design companies collaborate with third-party fabrication foundries to manufacture and test their integrated circuit designs. This allows design companies to rapidly develop new devices. They do not need to restructure their production chains for new designs and just focus on designing. Moreover, even small design houses can innovate without the substantial financial burden of investing in their own integrated circuit fabrication facilities.

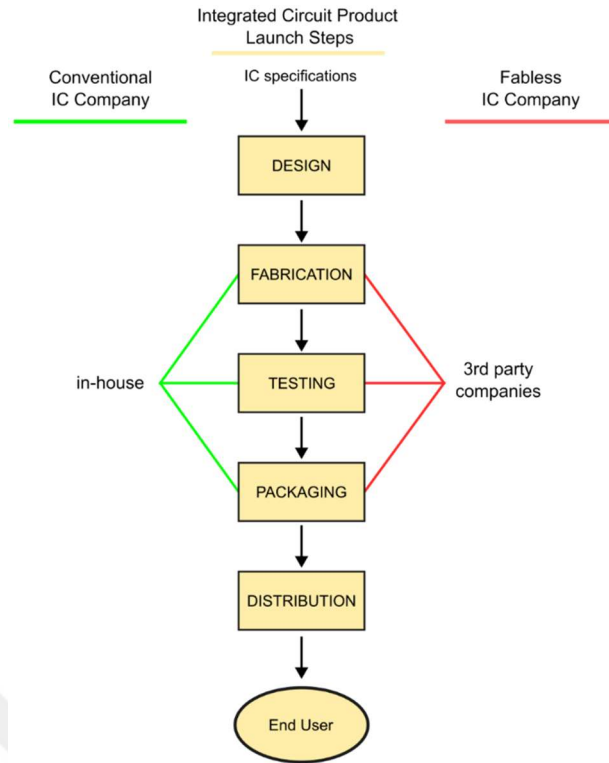


Figure 1: IC product launch steps difference between fabless and conventional IC company.

However, this comes with new issues. In the supply chain one or more partners can deceive the contract. This creates significant risks for product and intellectual property (IP) security. **Figure 1** shows production steps that have potential security risks because of the 3rd party companies which are necessary for fabless production. Rogue companies or employees may exploit their access to insert malicious modifications into products, steal proprietary designs, or produce unauthorized copies for their own benefit [1]. In the fabrication phase, designers send their design files to foundries for manufacturing. At this stage, the design becomes vulnerable to cloning or unauthorized overproduction. At the first glance it seems a great problem only for the designer company, but the issue can be even worse. Because effected devices may not only damage designers economically, but it can also risk the health of consumers, governmental system or military assets leading major risks on human life and national security. As reported in [2] a significant number of counterfeit components have been identified in defense systems. Importantly, these cases represent only the detectable incidents, while many counterfeit devices may go unnoticed. The presence of such unauthorized components in critical defense infrastructure can lead to system malfunctions, degraded performance, or even deliberate vulnerabilities that

compromise national security. Malicious ones can be waiting for their time to disrupt the crucial systems. Only increased awareness and necessary precautions can prevent such security risks.

There are extensive research and development for detection and prevention of security threats in digital circuits. [3] proposes a netlist level obfuscation method to protect the design. Obfuscation is based on antipiracy design flow for SoCs (System-on-a-Chip). It modifies pre-synthesized IP cores to maximize both structural and functional obfuscation while maintaining low design overhead without affecting end user. For cryptographic applications, [4] explains how PUF's can be used to authenticate ICs and generate volatile keys. PUFs uses circuit characteristics to generate volatile keys and enables authentication. It does not require expensive parts for authentication like EEPROM makes it cost-effective security application [5]. To combat IP piracy, [6] introduces an approach that uses combinational lock and public key cryptography (PKC). Manufactured integrated circuits (ICs) are embedded with unique identifiers and require unlocking through a key known only to the designer. To obtain the key, manufacturers need to send these IDs to IP rights holder. Hence, IP rights holder knows how many IC have been manufactured and prevent overproduction by manufacturer. One of the advantages of this approach is that it relies on already implemented commercial ICs, also it does not change design flow much and does not have significant power or delay overhead. With respect to analog, mixed-signal, and RF applications, security remains an underexplored topic. Existing security solutions for the analog domain are still in their infancy, with current implementations demonstrated only in a limited set of analog building blocks [6]. Because analog functionality is deeply embedded in many digital systems, these systems also become susceptible to security vulnerabilities. Semiconductor-level threats can lead to significant performance degradation in critical electronic systems [7]. As analog components are essential for enabling electronic devices to interface with the physical world, ensuring their security is vital to preserving their functionality and protecting overall system integrity. However, despite their critical importance, the design of analog circuits remains a highly manual and expertise-driven process, complicated further by the overlapping nature of specifications and design steps. Circuit design relies heavily on manual effort and expert knowledge, primarily because analog specifications and design steps often overlap, making it challenging to meet design constraints. [8]. It

requires careful consideration of multiple factors. Designers must account for all relevant aspects to ensure the functionality, reliability, and efficiency of the final device. Performance requirements, power consumption, area etc. usually define the design path. These factors often involve trade-offs among one another, which can be strategically leveraged during the optimization process. While these considerations primarily determine device performance, the growing threats to intellectual property (IP) security elevate security concerns to a level equally important as other design features. If designers fail to secure the device's operation or protect their ownership rights, the entire effort may be compromised. Consequently, it is essential for designers to integrate security aspects into the design process. In that case automation of circuit design should be combined with the security measures. Building trust in AMS/RF IPs requires close collaboration between researchers and industry to develop secure and reliable solutions [9]. Numerous defense measures have been developed to counter various types of attacks, including design locking to restrict usage to the owner, obfuscation of transistor sizes, manufacturing different design components across multiple foundries, and circuit marking. However, no single method offers complete protection against all forms of attack or guarantees unbreakable defense. Each approach presents its own vulnerabilities and limitations. As in many other fields of security, a continuous interplay between attackers and defenders persists, necessitating ongoing advancements in security techniques.

In this thesis, a comprehensive overview of security threats in integrated circuits is presented, covering issues such as intellectual property piracy, overproduction, recycling, reverse engineering, hardware trojans, and side-channel attacks. Subsequently, various defense mechanisms are discussed, including camouflaging, split manufacturing, watermarking, locking techniques, and physically unclonable functions (PUFs). Building on this foundation, we introduce a novel approach to security-aware optimization by integrating Particle Swarm Optimization with combinationally locked circuits, representing a unique methodology not previously explored in the literature. This approach is applied to two distinct analog designs—a two-stage amplifier and a bandgap reference—demonstrating its effectiveness in enhancing security while preserving functionality. The work concludes with recommendations for future research to further advance security in analog integrated circuit design.

2. BACKGROUND

This section provides an exploration of the current state of circuit design and automation, highlights common security threats faced by integrated circuits, and reviews developed defense mechanisms. These topics form the essential foundation for understanding and implementing security-aware optimization in analog circuit design.

2.1 Analog IC Design Automation and Optimization

Numerous optimization methods can be applied in automation. Successful integrated circuit optimization relies on the meaningful definition of constraints and the precise selection of objectives tailored to specific topologies. These elements guide the iterative optimization process toward feasible and effective solutions within the design space. Constraints are typically used to verify that circuit outputs remain valid and meaningful, while objectives aim to maximize or minimize particular performance specifications. In many cases, a single objective is insufficient to capture the full design goals; therefore, multi-objective optimization is employed to thoroughly explore the design space. This approach enables circuits to be fully utilized, ultimately revealing their maximum performance potential.

Optimization is categorized based on the number of objectives into three types: single-objective, multi-objective, and many-objective optimization. As the names suggest, the primary distinction among these categories lies in the number of objectives involved, often with conflicting goals. When optimizing a single objective, the process is called single-objective optimization. If exactly two objectives are considered simultaneously, it is termed multi-objective optimization. Finally, when more than two objectives are involved, the problem is classified as many-objective optimization.

Managing multiple objectives is fundamental to engineering practice. In integrated circuit design—and engineering problems in general—success often depends on effectively balancing trade-offs. Within optimization, these trade-offs are critical in selecting appropriate objectives. For instance, in a simple operational amplifier, gain and bandwidth typically exhibit conflicting behavior, making them suitable candidates for multi-objective optimization. Additionally, one might consider the impact of power

consumption on performance, thereby extending the problem to many-objective optimization with gain, bandwidth, and power consumption as simultaneous objectives.

Although most sub-blocks in electronic systems are digital ICs, analog components often dominate the design cycle in terms of time consumption, underscoring the importance of automating analog IC design [10]. The intricate design requirements of analog integrated circuits pose significant challenges to automation; nevertheless, substantial progress continues to be made in this field. Previous studies, such as [11], [12] rely heavily on expert knowledge and heuristic rules to address design challenges. While these approaches have demonstrated success, their dependence on domain expertise and their limited applicability reduce their practicality for general-purpose use. Recent approaches work with optimization algorithms that depend on machine learning, deep learning, and evolutionary algorithms. Reducing expert knowledge and the requirement for human intervention is one of the main goals of analog IC automation. **Figure 2** illustrates the general approach adopted for circuit design automation.

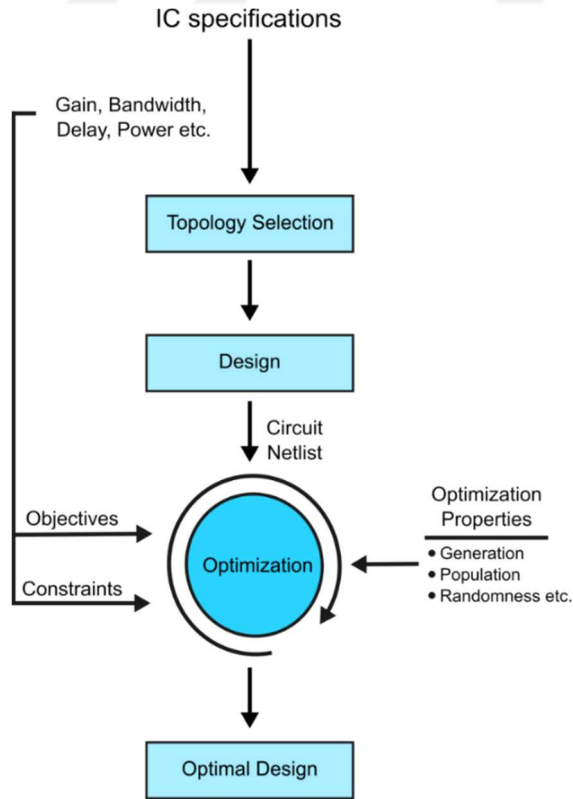


Figure 2: A general flow of circuit design automation.

Several recent studies have explored the application of machine learning and optimization techniques in analog IC automation. For instance, Deep learning was used to determine the optimum topology for desired circuit performance in [13]. It uses the relationship between circuit characteristics and topology to choose which topology can give the desired circuit specification between four different circuit topologies. In [14] researchers demonstrate fully automated synthesis from circuit-level specifications to a physical layout description. It utilizes multi-objective multi-constraint optimization methods to synthesize circuit.

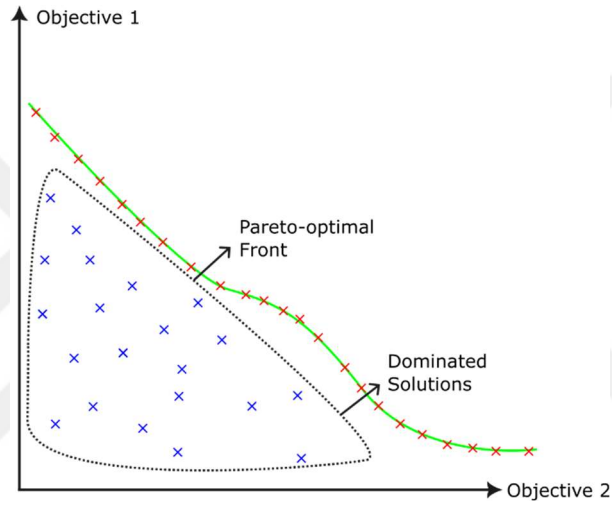


Figure 3: Pareto-optimal front for multi-objective optimization.

[15] utilizes SPEA2 algorithm to generate POFs (Pareto-optimal Front) for selected design problems. POF represents the set of solutions that are optimal across all objectives. In other words, it includes solutions that are not dominated by any other — meaning no objective can be improved without degrading at least one other. **Figure 3** illustrates an example of a POF, showing the trade-offs among two objectives. The idea is to find solutions for different topologies and create an analog library in the case of reuse of previously generated designs for various power and load needs. This approach enables designers to efficiently explore the design space by visualizing possible solutions in the objective space or by selecting a suitable design point to proceed further in the design flow. Similarly [16] compares two different multi-objective optimization method and explores design spaces for analog and RF circuits, showing different design possibilities for the selected optimization methods for

different topologies gives qualitative insight on both topologies and optimization algorithms.

2.2 Hardware Security and Trust

While circuit performance is undoubtedly critical, overlooking security can render the entire design effort ineffective. Throughout the different phases of a device's lifetime, a design can face to a range of distinct security threats [1]. During the design phase, hardware Trojans may be inserted; at the fabrication stage, design files can be intercepted or stolen; and once deployed, the device may be subject to reverse engineering and cloning. These threats are summarized in **Figure 4**.

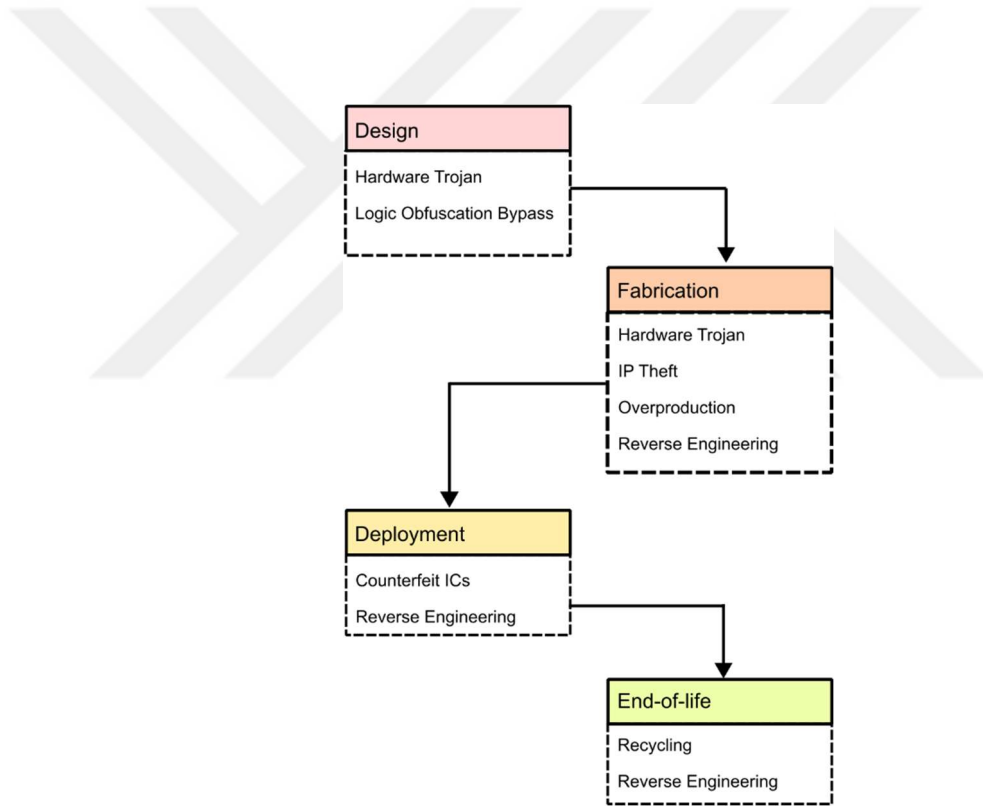


Figure 4: Threats through ICs lifetime.

Ensuring the security of a design is as important as the design process itself; however, the lack of awareness regarding hardware security poses significant risks throughout the supply chain [17]. IP theft and counterfeit devices lead to substantial economic losses. Beyond direct financial damage, cloned devices also erode brand value, posing an even greater challenge for the original design companies. Moreover, the infiltration of counterfeit components into authentic production chains has the potential to induce

malfunctions or suboptimal performance in the affected systems. While specific defense mechanisms have been shown to mitigate these threats, they cannot be entirely eliminated. Each threat must be addressed individually, as no universal solution exists. Effectively managing these risks requires a comprehensive understanding of both the threats and the appropriate countermeasures. This underscores the critical importance of hardware security and trust in modern electronic systems.

2.2.1 Threats

2.2.1.1 IP Piracy and Overproduction

IP piracy is exploitation of the trust to foundry. The possibility exists that a rogue foundry, or even a single employee, could steal the design and produce them for their own purposes [1]. This breach cannot be immediately spotted makes it dangerous for the designer company. The distribution of stolen designs in the market has the effect of undermining the commercial interests and competitiveness of the original designers.

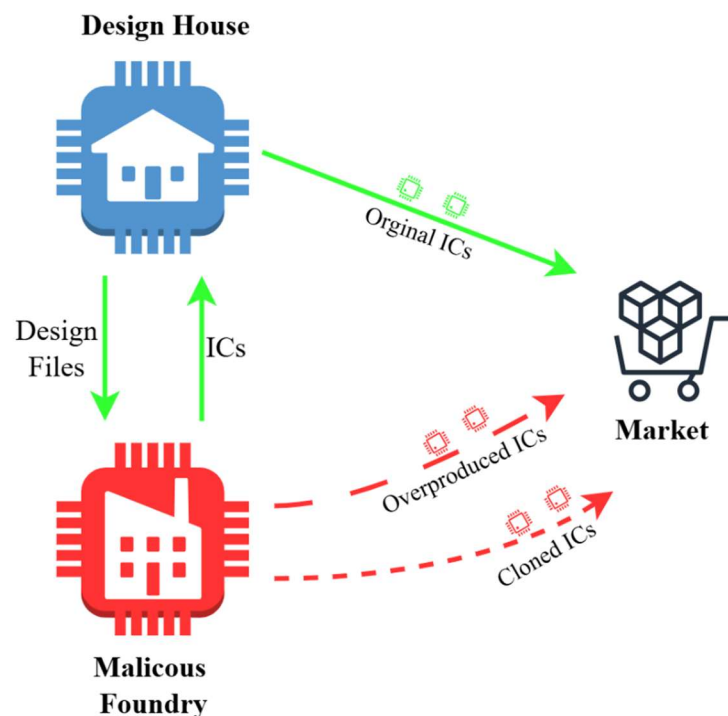


Figure 5: IC piracy and overbuilding.

Another potential threat posed by a rogue foundry is overproduction, in which the foundry manufactures additional devices beyond the authorized amount, rebrands them, and sells them independently, as illustrated in **Figure 5**. This type of threat does not require an expert designer. For most of the overproduction cases, attackers do not need to understand the functionality or internal architecture of the circuit. Instead, they leverage their access to design files which are necessary for the manufacturing process. Thus, they can easily produce additional unauthorized copies of the original design. These illegally produced extra devices are physically and functionally indistinguishable from original devices, which makes their detection difficult. In that case, these threats pose serious challenges to the integrity of supply chains.

2.2.1.2 Recycling

Recycling refers to the practice of using old or end-of-life products, rebranding them, and reselling them as fresh [17]. Attackers may obtain these obsolete products, harvest individual components, or redistribute them as complete units. This threat creates serious issues where unreliable devices on the market can cause serious malfunctions to many systems.

2.2.1.3 Reverse Engineering

Reverse engineering is the process of uncovering the technical details of intellectual property (IP) [1]. While, in theory, reverse engineering is not illegal and can be employed for legitimate research and development purposes, it can nonetheless harm the original designer. Replicating an innovation through reverse engineering is often significantly easier than the initial process of innovation, thereby providing an advantage to competitors who are otherwise lagging behind. When a company seeks to enter a new area of electronics, it may acquire an existing product, disassemble it to analyze its functionality, and gain insights into its design. By leveraging this understanding, the company can then develop its own version of the product [18]. Nowadays advance methods are more common which depends on reverse engineering of original devices. Readily available tools like Degate [19] gives opportunities for reverse engineering.

[20] presents a 2014 case of reverse engineering where an individual successfully cloned the Honda S300—a modification tool used to adjust parameters such as air-fuel

mixture, idle speed, and other settings directly affecting Honda vehicle performance. While cloning a printed circuit board (PCB) is relatively straightforward, replicating a microchip containing billions of transistors poses a significantly greater challenge, which was also achieved in this example. [21] illustrates another notable case of reverse engineering, where an IC is analyzed using an electrical circuit tester. During this process, detectors analyze the optical emissions from the circuit to extract timing information. The collected timing data is then compared with available model information to identify the specific circuits under test. This method is both easy to perform and cost-effective, making it a practical threat to circuit security.

Apart from its malicious uses, reverse engineering can also be employed for verification purposes, helping to detect unauthorized modifications introduced during the fabrication phase. In [22] an algorithm is proposed that identifies module boundaries within an integrated circuit and extracts their functionalities. This facilitates verification of the IC's integrity, highlighting the vital role of reverse engineering in today's globalized, multi-vendor manufacturing environment.

2.2.1.4 Hardware Trojans

Hardware Trojans (HT) are malicious entities deliberately embedded into integrated circuits by rogue employees or untrusted foundries. These hidden modifications can extract sensitive information without the knowledge of the original designer or disrupt the normal operation of a device [17]. Given their covert nature and potentially severe consequences, Hardware Trojans represent a significant threat to the security and reliability of electronic systems.

HTs can be activated through a range of triggers, including timing-based mechanisms, environmental conditions, remote signals, or a combination of these factors [23]. Detecting HTs can be particularly challenging, as the performance degradation they cause is often negligible compared to the natural variations introduced during the fabrication process. This subtlety makes analog circuits especially vulnerable to HT insertion, where distinguishing between legitimate variations and malicious alterations becomes difficult. In [24] it is demonstrated that an oscillator can sustain oscillations at multiple frequencies or amplitudes with only minimal changes to its energy storage elements.

Hardware Trojans poses great danger to many different areas. Malicious functions can be added to military devices. This way crucial and sensitive data can be extracted or completely disable critical system.

2.2.1.5 Side Channel Attacks

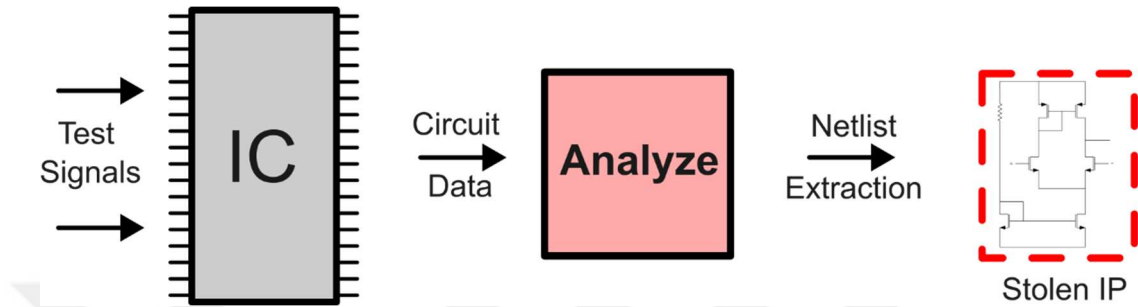


Figure 6: General scheme of a side-channel attack.

Side-channel attacks are a set of powerful techniques that exploit the physical structure and behavior of electronic systems to extract secret information, potentially compromising even otherwise robust security mechanisms [1]. The general scheme of a side-channel attack is illustrated in **Figure 6**. Side-channel attacks employ hardware-based techniques to compromise the integrity of secure systems, including cryptographic engines, protected memory structures, and isolated components [25]. One instance of a side-channel attack involves the implementation of power analysis techniques, such as Differential Power Analysis (DPA), on cryptographic systems. This method enables attackers to extract secret keys transmitted across internal buses without the need for physical tampering with the device. These attacks are not only non-invasive and difficult to detect, but also relatively inexpensive to carry out, making them an accessible and serious threat in practical scenarios [26]. With inspection of electromagnetic emanations from CMOS devices, another attack can be executed to extract information from secured systems. In [27] it is shown that even with a single-channel electromagnetic sensor, a lot of information can be extracted.

2.2.2 Defenses

2.2.2.1 Camouflaging

Camouflaging is a technique used to conceal transistor dimensions or circuit functionality at the layout level to prevent reverse engineering. With the combination of dummy and real contacts, designer can deceive the reverse engineer and protect the design presented in [28]. Another similar approach is presented in [29], where unused space in ASIC layout filled with special cells like the standard ones and connected with metals and vias establishes convincing visual and thus creating good camouflage effect.

Logic blocks can be utilized to camouflage a circuit. In [30], configurable logic blocks are employed to obscure the design. Various types of logic gates are constructed using identical building blocks, schematics, transistor connections, and ultimately the same layout. That makes them indistinguishable under microscopic inspection. The functionality of these logic blocks is controlled through external control signals, which allows the same physical structure to implement different logic functions.

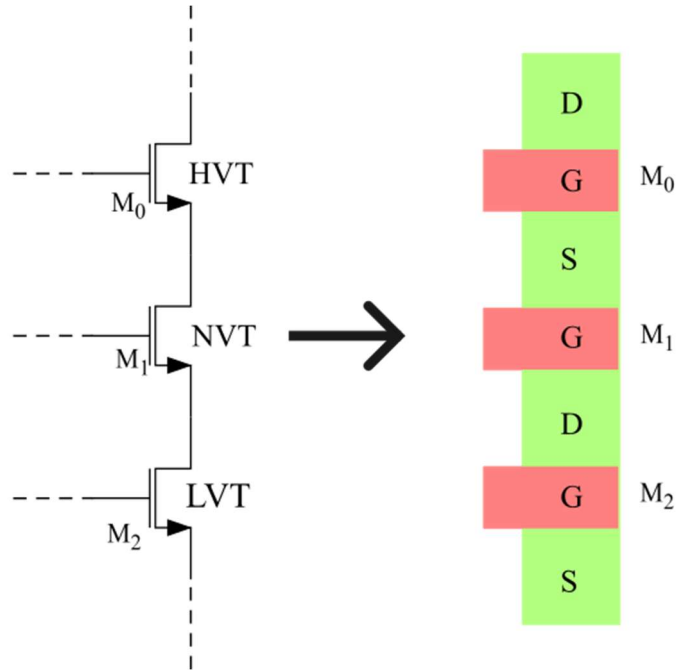


Figure 7: Transistors connected in series with varying V_t .

The performance of analog circuits is highly sensitive to threshold voltage variations. By exploiting this characteristic, multi-threshold transistors can be used as a means of camouflaging, effectively concealing circuit functionality [31]. Transistors threshold levels cannot be identified in reverse engineering process. Usually, PDKs provide three different threshold models which are LVT (Low V_t cells), HVT (High V_t cells), NVT (Nominal V_t cells). Consequently, the identification of individual transistors is dependent on the process of trial and error. Given the substantial interaction between transistors in analog designs, even a small number of camouflaged transistors can significantly complicate the task of distinguishing individual devices. Consequently, reverse engineering becomes a highly labor-intensive process, even for relatively small circuits. Splitting a single transistor increases the identification effort drastically. **Figure 7** illustrates a potential implementation of multi-threshold transistors, wherein three distinct transistor types are arranged in series, yet appear seamless at the layout level.

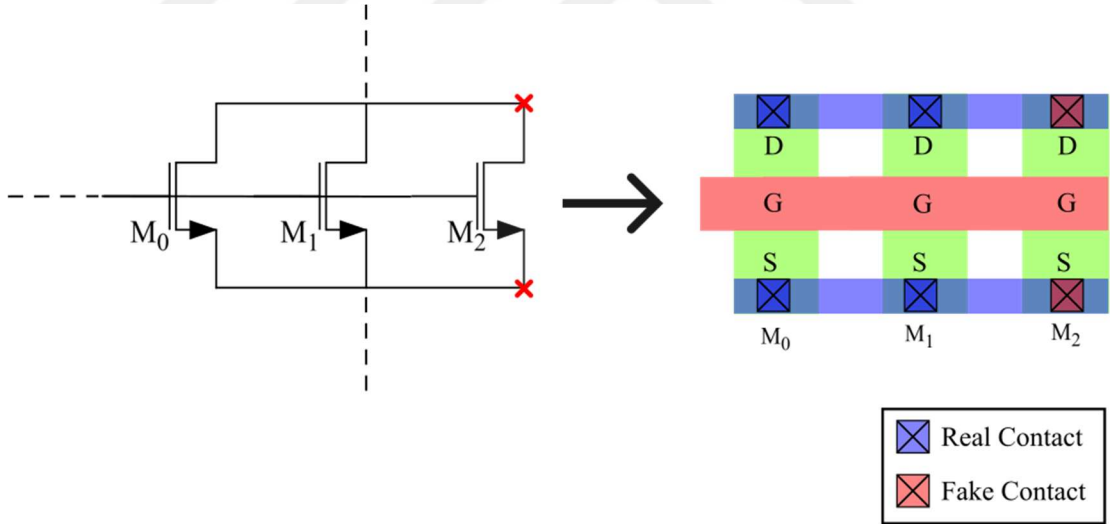


Figure 8: Fake contact example for transistors connected in parallel.

To enable the utilization of camouflaged transistors, [32] presents a library containing commonly employed components in analog layouts, which incorporate false contacts to safeguard the design against reverse engineering. Fundamentally, transistor sizing can be obfuscated by introducing additional fingers or using multipliers, followed by the insertion of fake contacts that create floating nodes. These fake contacts are

indistinguishable even under microscopic inspection, effectively concealing the true structure of the transistor. In **Figure 8**, the source and drain terminals of three transistors appear to be connected in the layout. However, through the use of fake contacts, the M2 transistor is effectively disconnected. Rather than having three transistors in parallel, only two transistors are actually connected.

There are some drawbacks to the utilization of camouflaging. When dummy transistors and contacts have been added, there will be loss on performance like power, area, delay [28]. However, this cost can be considered negligible compared to the benefits of protecting the design.

2.2.2.2 Split Manufacturing

Against untrusted foundries, split manufacturing methods have been developed. Layout of IC has been split between front-end-of-line (FEOL) and back-end-of-line (BEOL) [33]. Then two parts of the layout will be fabricated in different foundries. Initially, the designed layout is split into two pieces which are BEOL and FEOL. FEOL consists of transistors and lower metal connections and BEOL contains top connections. Without knowing connections at BEOL attackers cannot identify design to pirate [34].

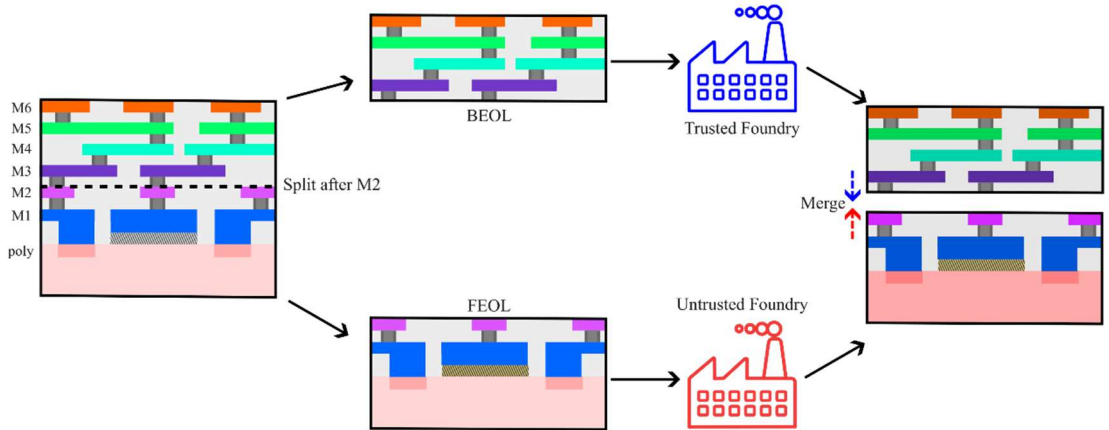


Figure 9: Example of split manufacturing scheme.

Split manufacturing is a relatively new method used to protect RF IPs from reverse engineering at the foundry stage [35]. In split manufacturing, different layers of an integrated circuit are fabricated at separate foundries, as shown in **Figure 9**. This

separation complicates the understanding of critical design elements, thereby reducing the risk of design theft or overproduction by any single foundry. Even though malicious foundries can obtain some degree of design details, with the absence of knowledge on critical parts and without knowing all of performance details makes it challenging to replicate the design.

Regarding performance and power consumption, [36] evaluates split manufacturing after the M1 layer and demonstrates that intellectual property protection can be efficiently achieved with minimal performance loss and only a slight increase in area. However, split manufacturing doesn't completely prevent rogue foundries from stealing design. Without additional protection, an attacker can obtain most of the BFOL connections. To mitigate this weakness, [34] suggests a swapping pin method. By swapping pins, BFOL identification will become harder for attackers to do correctly.

2.2.2.3 Watermarking

Watermarking is an identification technique in which the design is marked to demonstrate its originality. The watermark must be seamlessly embedded within the circuit to avoid disrupting the circuit's operation, while remaining hidden to prevent easy detection and removal by potential attackers. These characteristics make watermarking a viable solution for protecting intellectual property [1].

Increased use of reusable designs and easily integrable virtual components has made the security of these intellectual properties increasingly important. In [37] a constraint based non-intrusive watermarking method has been proposed to protect IP and support reutilization of design. The application utilizes constraints to designate the output of a given design, synthesis, or optimization, thereby protecting the intellectual property. [38] introduces a watermarking approach that leverages routing-level nets to embed ownership information into the circuit layout. The watermark is composed of randomly generated ones and zeros, and the number of bits indicates the number of nets in the circuit. The design owner utilizes a pseudo random number generator, feeding it with identifying seeds to generate a unique watermark. This watermark serves as a means of verifying the authenticity of the circuit, thereby ensuring its genuineness and preventing the circulation of counterfeit components.

However, when it comes to analog circuits, small transistor counts and less complex design make it harder to apply watermarking to them, showing less effectiveness compared to digital counterparts. [39] Proposes a watermarking technique for analog ICs that doesn't affect IP functionality and does not add any overhead.

2.2.2.4 Locking

Generally locking of the IC means that its functionality and performance are secured with some sort of key. Usually, keys consist of number of bits. Various locking mechanisms can be implemented in ICs. One application involves locks, where signals can be manipulated so that only with the correct key will the correct output signal be obtained. Another application is transistor-size obfuscation. In this approach, the physical dimensions of transistors are concealed to prevent attackers from inferring circuit function or parameters. An example of size obfuscation with vector-based configuration is shown in **Figure 10**.

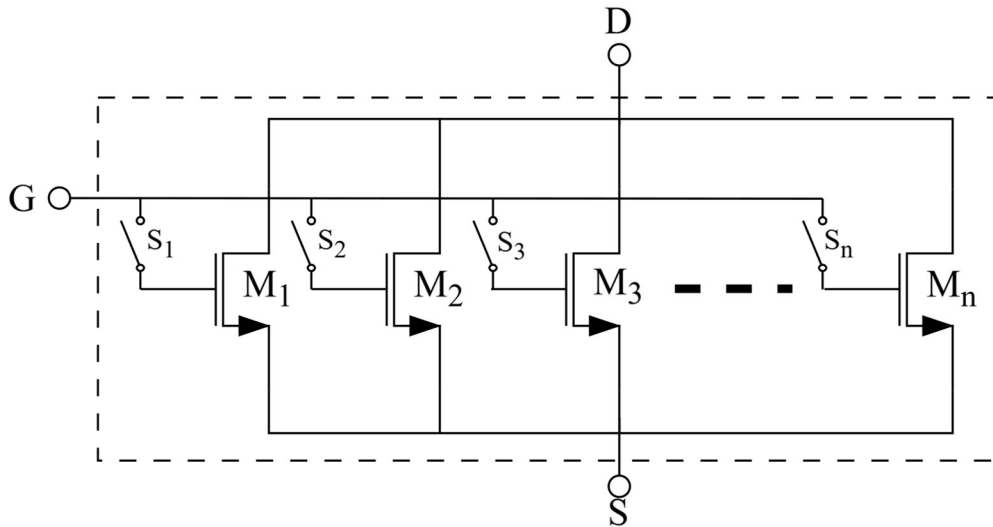


Figure 10: Size obfuscation with vector-based configuration.

Digital circuits are much easier to be secured with locking because digital operation can be completely disrupted with single bit. For the analog single and even a few key difference may give similar/acceptable responses [40]. This characteristic makes it challenging to create a design that operates correctly with a single working key. Although implementation is challenging, it remains a viable and effective technique.

Some key elements that affect the performance of the designs can be utilized to control the specific device. The performance of analog circuits mostly revolves around the current of the circuit. Most of the circuits' performance can be defined with the current that it flows.

[41] proposes a locking method which utilizes combinational locking on current mirrors of selected circuits. Instead of using parallel transistors to control current, proposed approach uses array of transistors. This array of transistors and their effect on performance of circuit, computed and solved using satisfiability modulo theories (SMT). This way only a single key value can make the circuit work on the desired specifications. SMT attacks also need to be considered. Since locking is implemented using SMT, it remains vulnerable to SMT attacks. However, these attacks require knowledge of current values, which are typically not directly accessible unless under carefully designed test benches. This requirement makes cracking the code more difficult, though not impossible. Overall, this approach primarily aims to prevent reverse engineering and recycling, while also providing some protection against breaches originating from the foundry. Another locking approach is presented in [42] where two different method are implemented and compared on two different circuit. The locking mechanisms are based on parallel transistors and meshed transistors, each designed to control circuit performance. In the parallel transistor configuration, circuit sizing is controlled along a single dimension, whereas the mesh configuration enables two-dimensional control over branch currents. An example of the mesh configuration is shown in **Figure 11**. The test circuits used are a basic two-stage amplifier and a bandpass filter. The introduction of locking alters the circuit behavior, causing performance to deviate from the desired specifications, necessitating a re-tuning process. After re-tuning, SMT algorithms are employed to determine the appropriate sizing for both locking configurations, such that the circuits function correctly only with the correct key. After configuration, several tests carried out with corner analysis and results are promising for the usage of both parallel and mesh configuration.

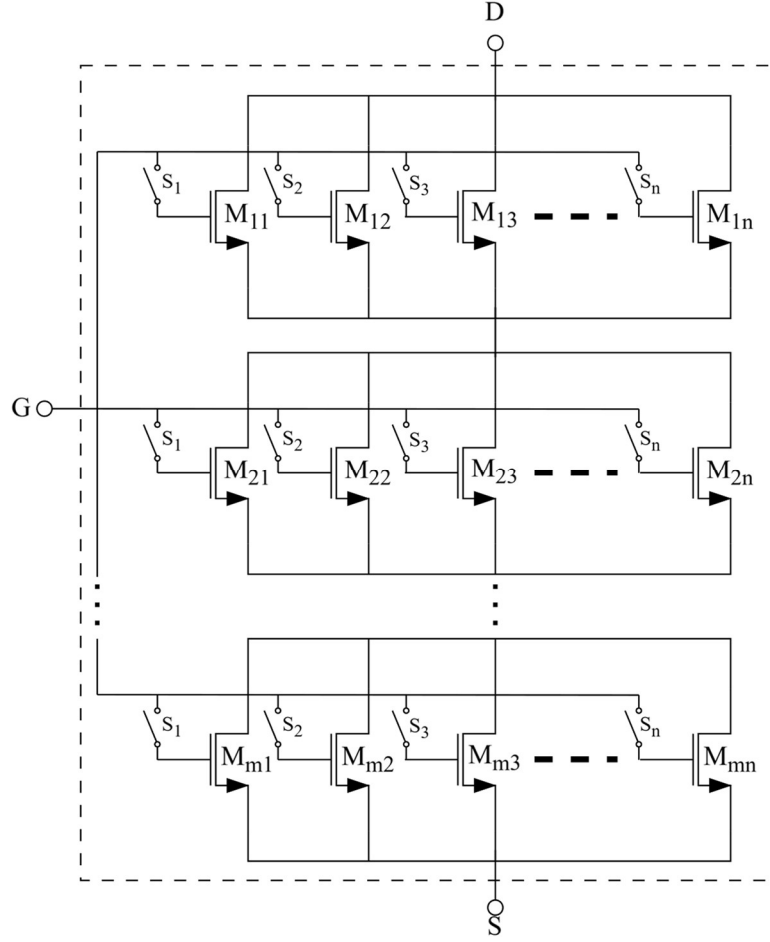


Figure 11: Sizing obfuscation with mesh-based configuration.

[43] utilizes floating gate transistors and analog neural network to obfuscate the biasing voltage of LNA. Trained analog neural network gives correct bias only when the correct key is input. Strong part of this approach is usage of floating gate transistors enables to define the key in continuous space gives lots of possibility for the correct key making harder for attacker to guess. It also defends itself against model approximation attacks.

To enhance the security of programmable analog integrated circuits (ICs), [44] proposes a method designed to protect circuits against a wide range of security threats. A key advantage of this approach is that it does not require any modification, tuning, or redesign of the original circuit, and most importantly, it introduces no performance degradation. Furthermore, it preserves the power consumption profile of the analog IC by focusing solely on modifying its calibration mechanism. Calibration mechanisms are typically employed to compensate for process variations, mitigate non-idealities,

support different operational modes, or adapt to environmental changes. In this method, a locking scheme is applied to the programmable fabric of the calibration mechanism, ensuring that only the correct configuration can enable proper operation. If an incorrect calibration is attempted, the circuit will either malfunction or demonstrate suboptimal performance. Provided that the calibration configuration remains confidential, this approach offers a highly effective means of securing analog ICs without compromising their performance.

[45] presents a key-based logic encryption and emphasizes the difficulties when implementing locking mechanisms to high frequency systems such as phase locked loop (PLL) where small differences and increased parasitic affect performance highly and points out its requirement of optimization. Implemented technique can be used in many analog parts of the system to improve resilience against attacks yet added parasitics should be considered and handled carefully.

In [46] Bandpass filter (BPF) has been secured using logic locking by controlling operation of optimizer. With optimizer and tuning knobs values of resistors can be tuned to get desired frequency. When the key is given as input to the optimizer, it checks within the tamper proof memory. If the input key and knob values are correct circuit can be tuned as desired. If the input key is incorrect, the optimizer produces undesirable response thus deteriorates the performance of the circuit. The proposed method is then extended to other circuits, including a Low Noise Amplifier (LNA) and a Low-Dropout Regulator (LDO), demonstrating its applicability to another analog circuits.

For RF transceivers [47] proposes a method that utilizes Stripped Functionality Logic Locking (SFL)-rem to implement logic locking to digital blocks in the signal path. Without the correct key, the analog signal becomes distorted, and proper signal propagation is only achievable when the correct key is supplied.

2.2.2.5 Physical Unclonable Functions

Physical Unclonable Functions (PUFs) are utilized to generate volatile secret keys based on intrinsic circuit characteristics, thereby eliminating the necessity to store keys within the integrated circuit. These secrets are only accessible while the device is powered on, thereby enhancing security against invasive attacks. PUFs generate secret

keys based on inherent circuit characteristics that emerge due to manufacturing variations. This results in device-specific secrets that are inherently difficult to predict or replicate. The generation of secret keys while the device is on rather than static keys present on the chip presents a more difficult challenge to the attacker [4].

PUFs can be separated into two categories which are weak and strong PUFs. Weak PUFs uses physical variations and fixed challenges to authenticate the circuit which is suitable for identification. Strong PUFs utilize process variations and are capable of accepting numerous challenge inputs, each yielding a unique response which makes strong PUFs more fitting for strong authentication [17].

Various implementations of PUFs have been developed within the analog domain. [48] presents a PUF which uses current differences that are caused by mismatched transistors to generate secret keys. In [49], a weak PUF proposed that utilize a voltage-compensated PTAT voltage generator to produce secret keys. The proposed method has been demonstrated to achieve VDD scalability down to 0.6V, thereby ensuring its viability as a cost-effective solution for energy-constrained applications. [50] converts leakage currents into secret keys with low power consumption and high speed. It has been demonstrated that, even under conditions of extreme temperature variations and supply voltage fluctuations, the error rate remains as low as 3%.

3. SECURITY AWARE OPTIMIZATION

The growing demand for rapid design processes has increased the importance of automation tools and optimization methods. As the design process becomes more streamlined, it is essential that security considerations advance alongside these developments. The main goal of this thesis is to create a system that successfully handles both performance and security needs.

IC automation and security are both relatively less studied in the analog domain. Even though analog ICs are the backbone of many electronic systems, they have not received as much attention in terms of security compared to their digital counterparts. Analog characteristics cause similar difficulties for advancement on both automation and security. Although a lower transistor count may seem to simplify automation, utilizing such minimal-transistor analog designs is significantly more complex than digital counterparts due to the nonlinear behavior of analog circuitry and the complex performance considerations it requires. Lesser transistors count also becomes another issue when we look at it from a security perspective. Sparse transistors in analog circuits make it easier to examine and understand most of the analog circuitry under the right conditions makes it very vulnerable to reverse engineering and counterfeit IC. By contrast, for digital circuits, it is more convenient to implement locking mechanisms. This is primarily because concealing design details or implementing hardware locking mechanisms becomes significantly more feasible in devices with millions or even billions of transistors, where such additions can be integrated without noticeably impacting functionality.

In order to achieve optimization with an awareness of security, it is necessary to develop an automation scheme that optimizes the circuit while also accounting for its security aspects. This adds heavy weight on optimization difficulty. Each added security mechanism inevitably affects, at the very least, the DC characteristics of the circuit. Especially on low power applications little disturbances on DC points may result in great differences in the complete operation of the device.

3.1 Defense: Locking

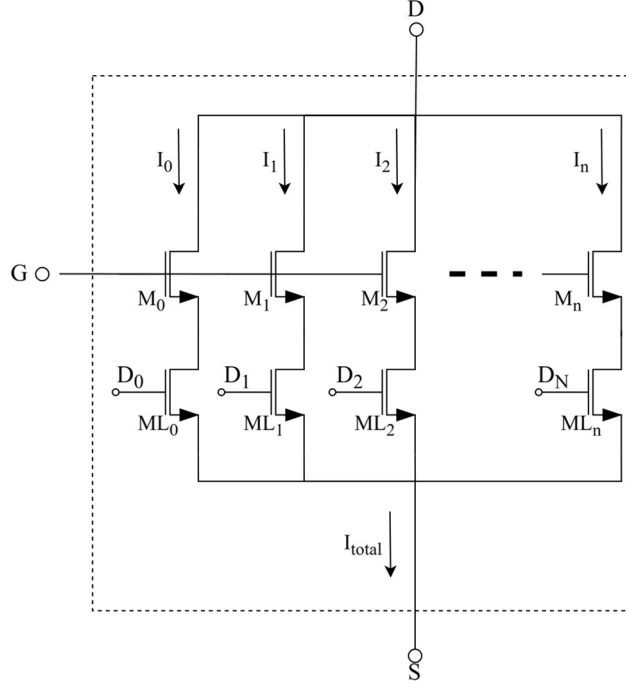


Figure 12: Combinational locking implementation.

Implementation of combinational locking method was given in **Figure 12**. Transistor size is obfuscated using n number of parallel transistors and controlled with n number of transistors in series with control bits which represented with D . Total amount of current that flows from effective transistor represented by I_{total} and can be defined as:

$$I_{total} = \sum_n D_n I_n \quad (3.1.1)$$

Combinational locking methods generally aim to control the sizes of some or all of the transistors and create secure devices against reverse engineering, overproduction, and IC cloning. With combinational locking, a designer can control the current that flows on a transistor, or voltage drop on specific branch. With this approach, design performance can be controlled with specific key combinations.

3.2 Optimization: Particle Swarm Optimization

There are several optimization models that can be used for circuit design automation. One of the most common ones is the Particle Swarm Optimization (PSO). Particle swarm optimization is optimization of continuous nonlinear functions [51]. An illustration of Particle Swarm Optimization is shown in **Figure 13**. Analog circuits are typically nonlinear in behavior, making PSO a suitable choice for circuit optimization due to its effectiveness in handling continuous and nonlinear objective functions. Also, PSO uses simple concepts that make it easier to implement with low cost. It requires simple mathematical operation, inexpensive memory requirements and low computational power. The generation of data for circuit optimization is typically accomplished through SPICE simulations, and the ease of optimization significantly enhances the overall efficiency of this process.

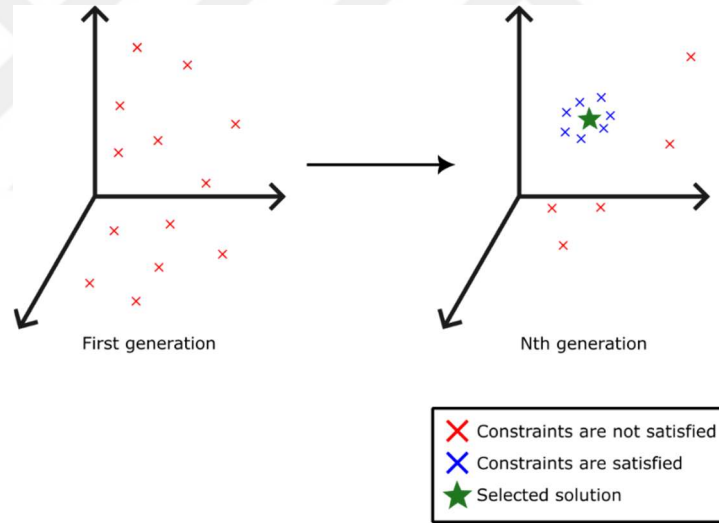


Figure 13: Particle swarm optimization.

Implementation of Particle Swarm Optimization achieved with variation of original method Adaptive Particle Swarm Optimization [52] and using PYMOO framework [53]. Each particle's velocity has been influenced by global and local best solution. Particle velocity has been defined as:

$$V_d^i = \omega V_d^i + c_1 r_1 (P_d^i - X_d^i) + c_2 r_2 (G_d^i - X_d^i)$$

And position value has been expressed with:

$$X_d^i = X_d^i + V_d^i$$

The parameters used in these equations are listed in **Table 1**.

Table 1: Particle Swarm Parameters

X_d^i	d-th coordinate of i-th particle's position
V_d^i	d-th coordinate of i-th particle's velocity
ω	Inertia weight
P_d^i	Position with best fitness for i-th particle
G_d^i	Best position globally
r_1, r_2	Independently generated uniformly distributed two random numbers
c_1, c_2	Acceleration coefficients

3.3 Attack model: Brute Force

Locked circuits with smaller key sizes are inherently more vulnerable to brute-force attacks. To assess the security of the circuits, a commonly used brute-force attack model was employed. In this approach, all possible key combinations for the locked circuit were simulated, and the resulting outputs were evaluated. For instance, the brute-force attack on a 6-bit locked circuit is summarized in **Figure 14**. In the case of a 6-bit key, a maximum of 64 simulations may be required to identify the correct key. Evaluating performance under these conditions necessitates testing all possible key combinations.

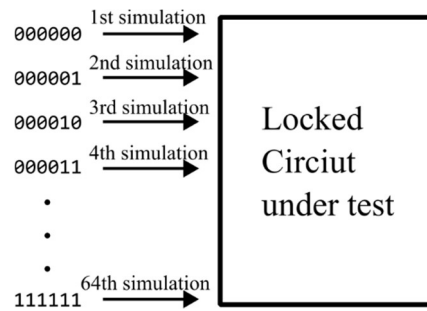


Figure 14: Brute force attack for 6-bit lock.

4. PROPOSED APPROACH

In our proposed approach, security-aware optimization is introduced by combining particle swarm optimization (PSO) with combinational locking techniques. Particle swarm optimization has gained significant popularity in circuit optimization due to its efficiency and adaptability, while combinational locking provides a straightforward mechanism to enhance security in analog circuits. By combining two, it enables to create security aware optimization. When optimizing a circuit, it is crucial to carefully select objectives that effectively guide the search for an optimal solution. Common objectives include power consumption, performance metrics, and area. For example, minimizing power is particularly important in battery-operated systems, while meeting specific performance requirements ensures the circuit functions as intended. Nevertheless, when security concerns are taken into account, the objective function must undergo modification to align with these supplementary priorities.

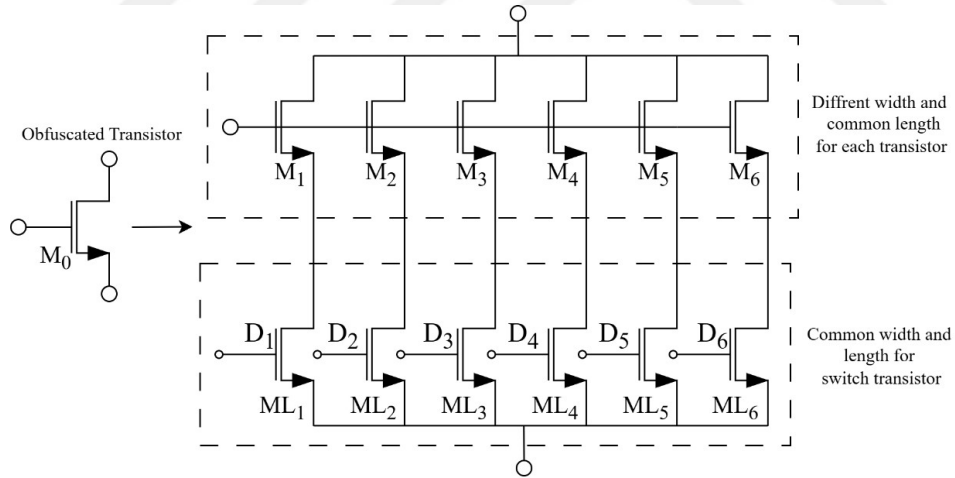


Figure 15: Obfuscation of selected transistor.

To securely optimize the circuit, first combinational locking was implemented to obfuscate sizes of transistor of the selected designs. The obfuscation is achieved through the division of selected transistors into six parallel devices. The circuit is required to have an additional transistor for the design and locking mechanism as switches. Locking switches are controlled by different input signals. Switch transistors

are sized equally for each individual circuit while main transistors widths are parameterized. The locking scheme is summarized in **Figure 15**.

Constraints and objectives will be different for distinct types of circuits. Selection of objectives mainly revolves around that criticalness of that specific performance metric. For example, for an amplifier circuit gain or bandwidth is critical, making it perfect for to be selected as objective. For bandgap reference circuits the most important thing is the output voltage or temperature coefficient (TC). Because if the output voltage is incorrect, it doesn't matter if it has good power supply rejection (PSR) or good TC.

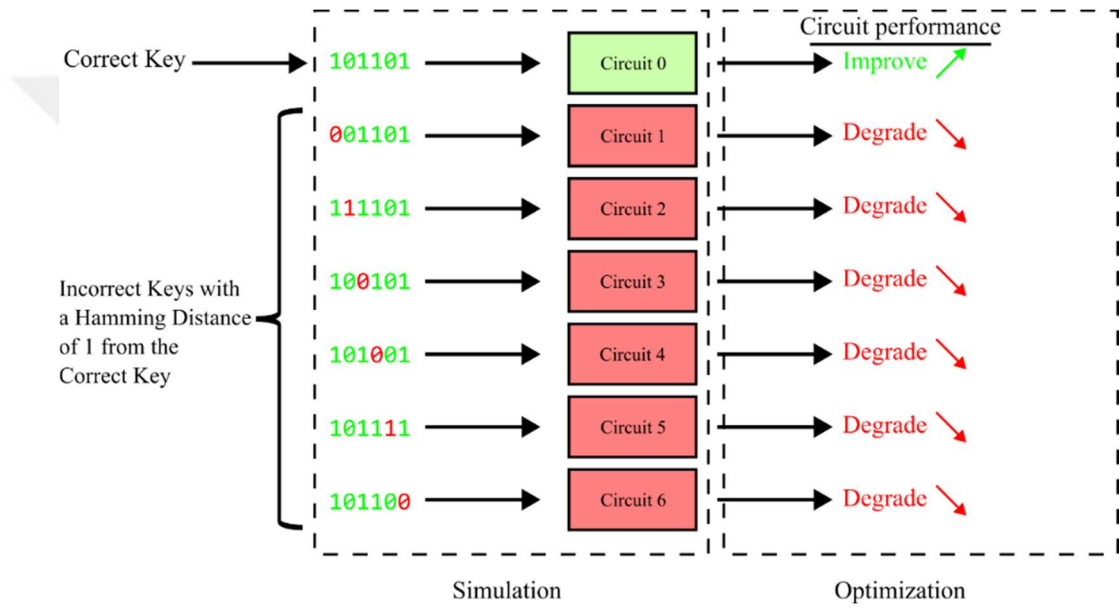


Figure 16: Security aware optimization.

After the implementation of security, the main idea of proposed approach is to maximize the error of specific performance metric. To achieve this, circuits unlocked with incorrect keys are included in the optimization process. These incorrect keys have a Hamming distance of one from the correct key. The objective is to maximize the performance of the correct key while degrading the performance of circuits with incorrect keys. This ensures that even a single-bit error in the key will produce errors at the output. A summary of the general scheme is presented in **Figure 16**

Constraints are key for correct design. Design specifications of desired circuits should be defined as the constraints of optimization. However, this process can also present significant challenges, as establishing constraints requires prior knowledge of the

design. While this requirement is generally considered unfavorable, it can be effectively managed by employing suitable methodologies. Optimization run without security elements can give certain clue performance space of the selected design. Security elements can also be leveraged to enhance circuit performance. By exploring different configurations, the effects of locks on performance, potential performance gains and losses, and ultimately the results of security-aware optimization will be investigated.



5. CASE STUDIES

In case studies, two analog circuits were selected: a two-stage amplifier, which is a common sub-block in many designs, and a bandgap reference, which is a critical circuit for reliable operation. Both circuits have been optimized without any security measures to establish baseline performance for the chosen technology, configuration, and topology. Next, conventional combinational locking has been applied, and the locked circuits have been re-optimized using the same cost function (i.e., without incorporating security terms). Then, the results have been analyzed to evaluate both performance trade-offs and the impact of locking on security resilience.

In the following step, a dedicated cost function will be constructed for security-aware optimization. For the selected circuits' wrong keys performance specifications will be deliberately degraded under incorrect keys, ensuring that only the correct key maintains desired behavior, while wrong keys force the circuit to perform significantly worse.

Two different types of optimizations are performed on both circuits, namely *Partial Optimization* and *Full Optimization*. In *Partial Optimization*, only the transistors responsible for locking the circuit are targeted, using the previously obtained sizes from the design without security. In *Full Optimization*, all transistors in the circuit are resized. **Figure 17** provides a summary of the flow of the case studies.

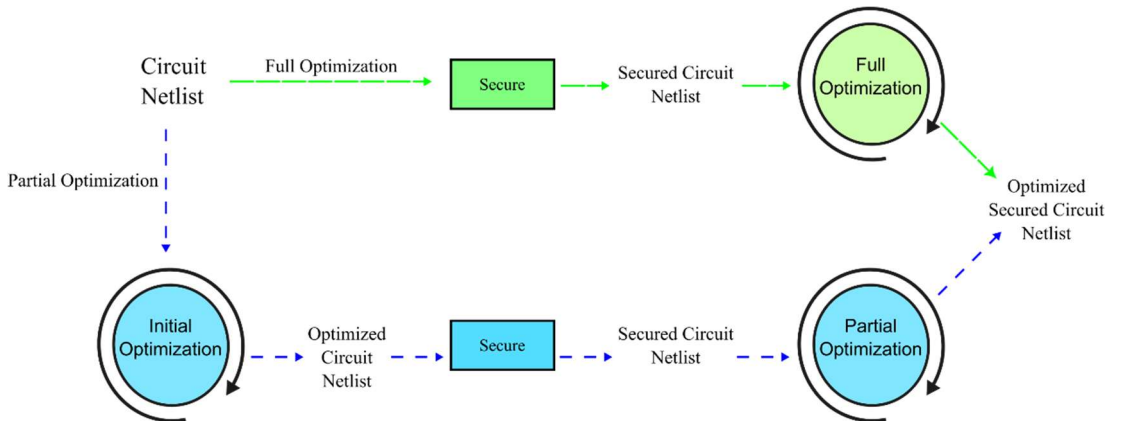


Figure 17: Flow of case studies.

5.1 Two-stage amplifier

The two-stage amplifier (TSA) was selected as the case study. For performance optimization, the TSA’s gain and phase margin were maximized, while power consumption and area were minimized. The 3 dB bandwidth is constrained within a specified range. For security optimization, the gain of instances unlocked with incorrect keys having a Hamming distance of 1 was minimized. **Table 2** shows the details of the optimization.

Table 2: Optimization properties.

Gen. Count	Swarm Size	Objective	Constraints			
			Gain	3dB Bandwidth	Phase Margin	Power
600	70	Minimize Cost Func.	60	15000-30000	45	1mW
1200						

5.1.1 Optimization of Two-Stage Amplifier (without security)

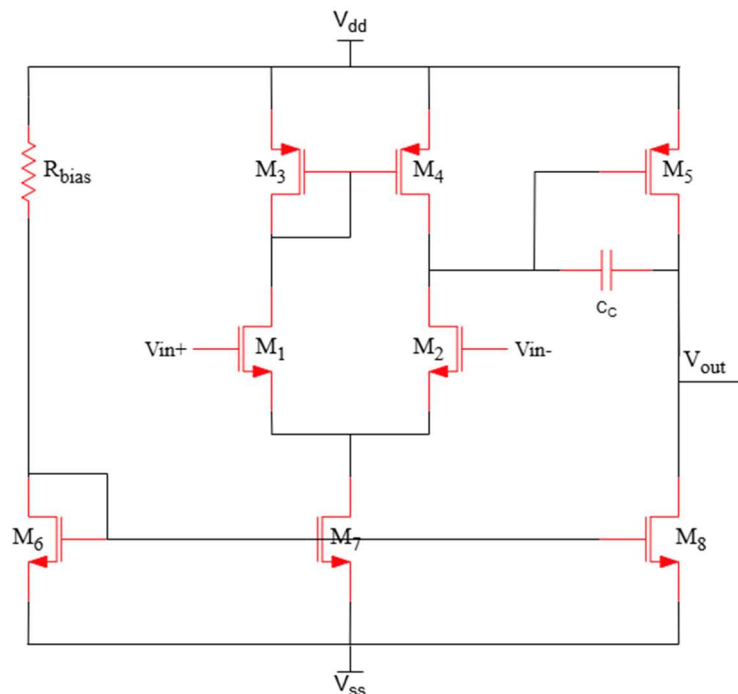


Figure 18: Two-stage amplifier. Components shown in red are included in the optimization process.

To analyze and determine the potential performance specifications of the selected two-stage amplifier topology, the schematic shown in **Figure 18** is constructed. For the optimization process, the particle swarm optimization (PSO) algorithm is employed with a swarm size of 70 over 600 generations.

The cost function simplified in Equation 5.1.1 is employed, with the objective of minimizing its value. The goal is to minimize power (P) consumption and area (A), while maximizing gain (A_v), phase margin (PM), and bandwidth (BW). All parameters are normalized to ensure equal influence on the cost function. The average cost corresponding to solutions that satisfy all constraints is plotted in **Figure 19**.

$$Cost = \left[\frac{(c_1 P_{norm} + c_2 A_{norm}) - (c_3 A_{v_{norm}} + c_4 PM_{norm} + c_5 BW_{3dB_{norm}})}{c_1 P_{norm} + c_2 A_{norm}} \right] \quad (5.1.1)$$

$$c_1 = 1, c_2 = 4, c_3 = 0.4, c_4 = 0.4, c_5 = 0.2$$

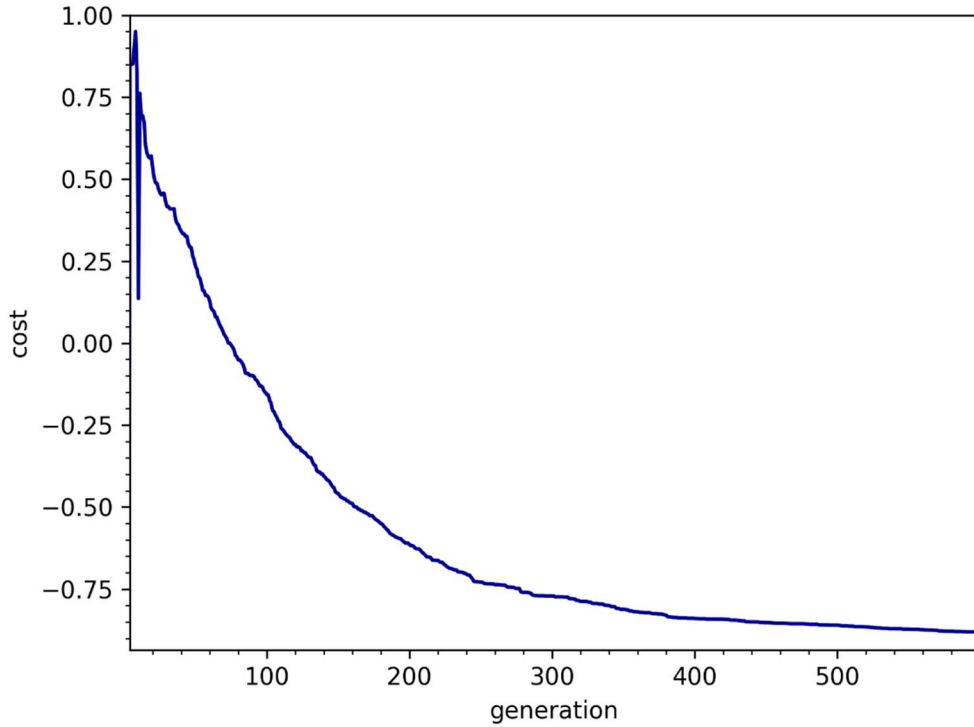


Figure 19: Average performance cost of TSO amplifier.

Table 3 presents the performance of the best member after 600 generations of performance optimization.

Table 3: Performance specifications of the best member after 600 generations of performance optimization.

Gain	Convergence Point	3dB bandwidth	Phase margin	Power	Area
60.8541dB	588	27.010k	67.40°	107uW	126.6um ²

5.1.2 Partial Optimization of Two-stage amplifier with 8-bit lock

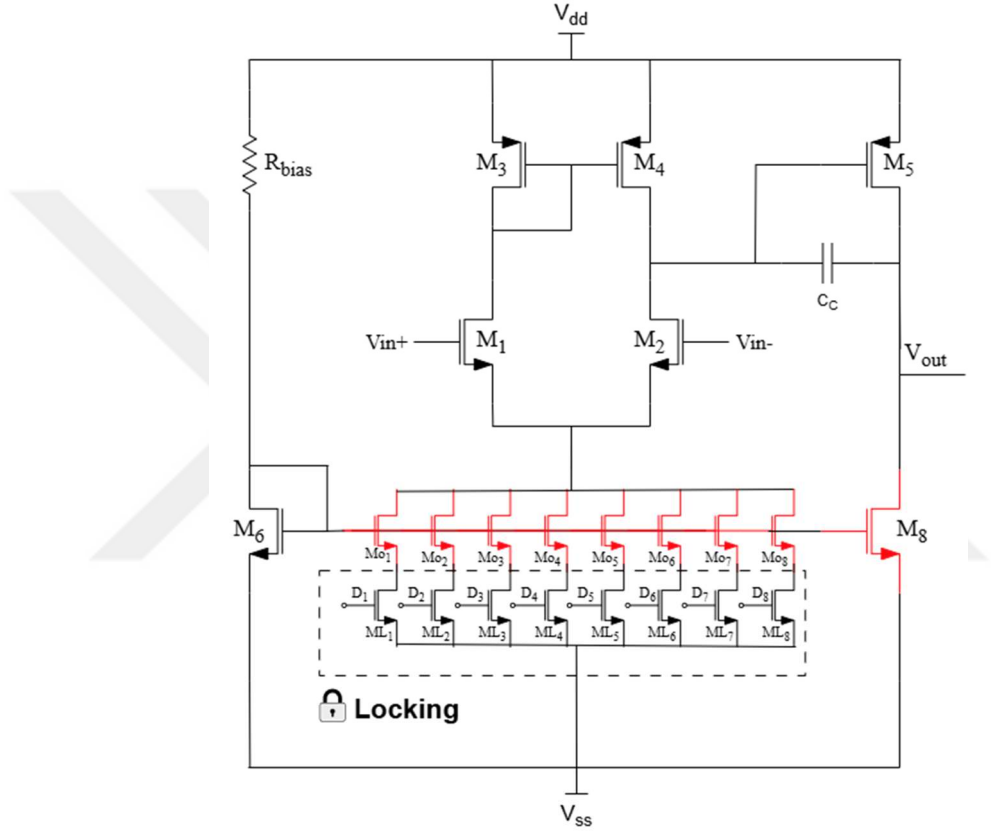


Figure 20: Two-stage amplifier with 8-bit lock. Transistors shown in red are included in the optimization process.

5.1.2.1 Performance optimization

In this case, an 8-bit combinational lock is introduced into the circuit, as shown in **Figure 20**. The transistors highlighted in red are optimized solely for faster convergence, with minimal impact on the performance of the rest of the circuit. Two distinct runs were conducted to evaluate the impact of the generation count, 600 generation and 1200 with the details summarized in **Table 2**. The simplified cost function is provided in equation 5.1.2. The circuit is optimized with the correct key to

meet the performance criteria and achieve improved results without considering security aspect. The average cost functions for the combined performance and security optimization are presented in **Figure 21** and **Figure 22**.

$$Cost = \left[\begin{array}{c} (c_1 P_{norm} + c_2 A_{norm}) - \\ (c_3 A v_{norm} + c_4 P M_{norm} + \\ c_5 BW_{3dB_{norm}}) \end{array} \right] correct_key \quad (5.1.2)$$

$$c_1 = 1, c_2 = 4, c_3 = 0.4, c_4 = 0.4, c_5 = 0.2$$

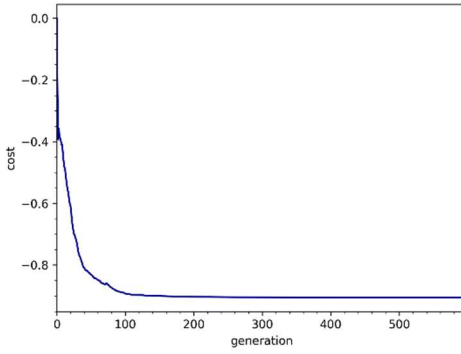


Figure 21: Average Performance Cost of TSO Amplifier with 8-bit Lock (600 generation)

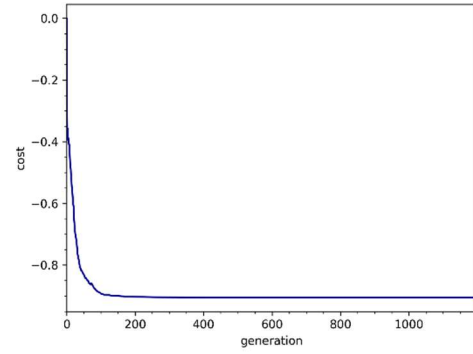


Figure 22: Average Performance Cost of TSO Amplifier with 8-bit Lock (1200 generation)

Table 4: Performance specifications of the best member after 600 and 1200 generations of performance optimization.

Gen. Count	Convergence Point	Gain	3dB bandwidth	Phase margin	Power	Area
600	154	60.696 dB	30k	71.7063°	122.7uW	159.3um ²
1200	154	60.696 dB	30k	71.7063°	122.7uW	159.3um ²

When the specifications in **Table 3** and

Table 4 are compared, both circuits exhibit similar performances. The circuit with the security feature shows increases in power and area due to the added obfuscation transistors.

5.1.2.2 Security evaluation of performance optimization

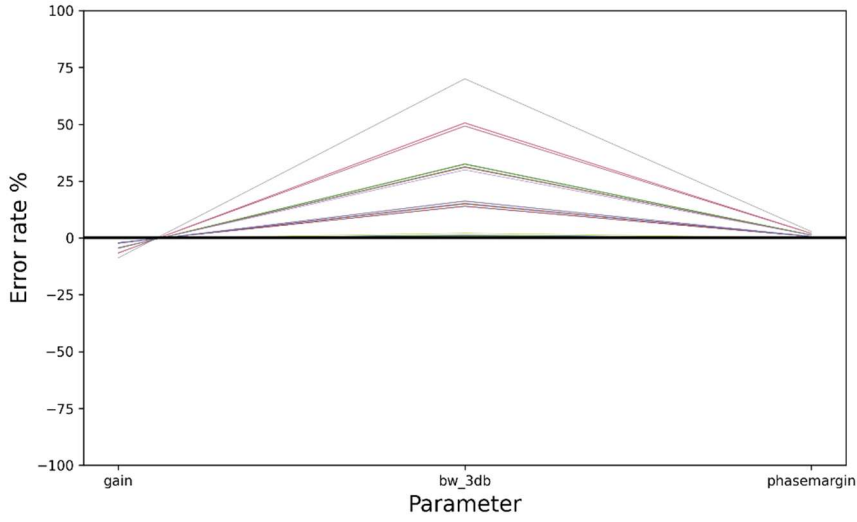


Figure 23: Error rates for each incorrect keys (56) satisfying the threshold after 600 and 1200 generations.

After selecting the best candidates from the optimization results, a security evaluation was conducted. For 600 and 1200 generations, 56 keys satisfy the performance criteria, as shown in **Figure 23**. Even though the performance requirements are met, the large number of falsely accepted keys suggests that the optimization process requires further refinement.

5.1.2.3 Performance and security optimization

In order to improve security, a new cost function was established, as presented in Section 5.1.3, combining the performance cost with a security cost. To enhance security, the circuit instances unlocked with keys having a Hamming distance of 1 included in optimization. These instances are optimized to exhibit degraded performance, specifically reduced gain, in this case. The optimization was then carried out using this combined cost function. **Figure 24** and **Figure 25** illustrate the average cost function for combined performance and security.

$$\begin{aligned}
\text{Performance Cost} &= \left[\frac{(c_1 P_{norm} + c_2 A_{norm}) - (c_3 A v_{norm} + c_4 P M_{norm} + c_5 B w_{3dB_{norm}})}{\text{correct_key}} \right] \\
\text{Security Cost} &= \left(\sum_{n=1}^8 A v_{norm_{ham_dis_1_n}} \right) / 8 + \left(\sum_{n=1}^8 P M_{norm_{ham_dis_1_n}} \right) / 8 \\
c_1 &= 1, c_2 = 4, c_3 = 0.4, c_4 = 0.4, c_5 = 0.2 \\
\text{Combined Cost} &= \text{Performance cost} + \text{Security cost} \tag{5.1.3}
\end{aligned}$$

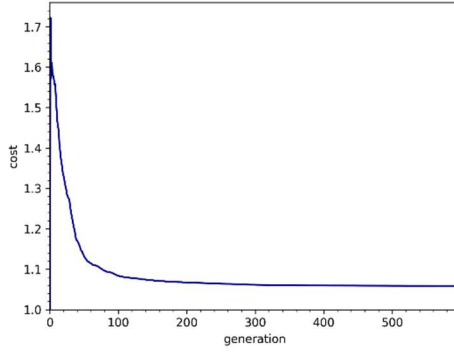


Figure 24: Average Performance + Security Cost of TSO Amplifier with 8-bit Lock (600 generation)

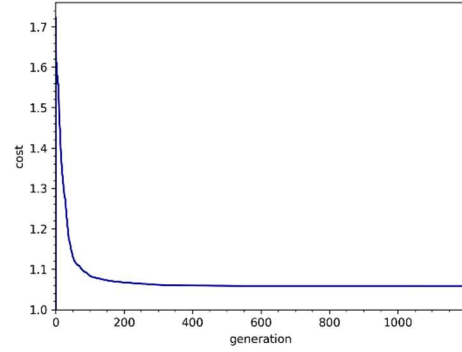


Figure 25: Average Performance + Security Cost of TSO Amplifier with 8-bit Lock (1200 generation)

Table 5: Performance specifications of the best member after 600 and 1200 generations of performance and security optimization.

Gen. Count	Convergence Point	Gain	3dB bandwidth	Phase margin	Power	Area
600	295	62.3488dB	30k	62.822°	154.8uW	279.9um ²
1200	295	62.3488dB	30k	62.822°	154.8uW	279.9um ²

Table 5 shows the performance of the two circuits corresponding to the best candidates after 600 and 1200 generations of combined security and performance optimization. The resulting circuits meet the desired performance criteria, with increased power consumption. This increase may be attributed to the weight of the security cost, which is absent in the performance-only optimization.

5.1.2.4 Security evaluation of performance and security optimization

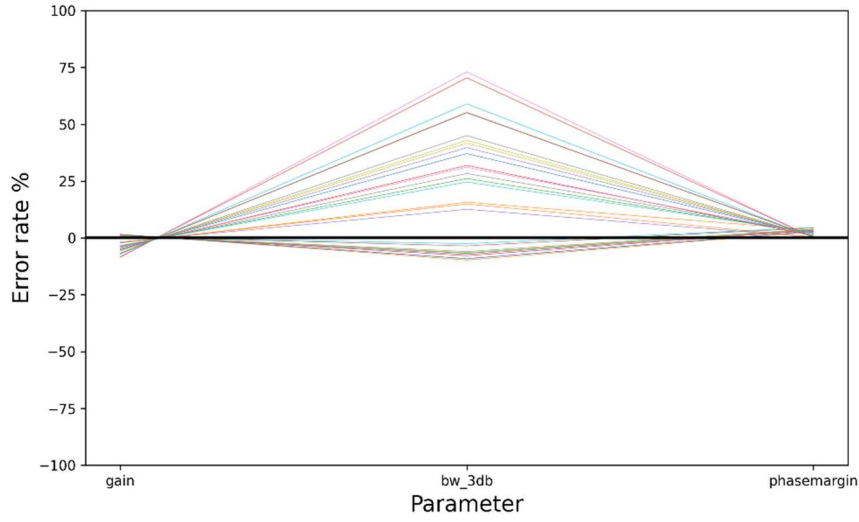


Figure 26: Error rates for each incorrect keys (28) satisfying the threshold after 600 and 1200 generations.

Security results are presented in **Figure 26**, illustrating the number of incorrect keys that satisfy the performance criteria. A total of 28 such keys were observed for both 600 and 1200 generations. With the security update applied to the cost function, the number of falsely accepted keys decreased from 56 to 28. Although this represents a significant reduction, it still cannot be considered sufficiently secure to be deemed successful. This limitation may be due to the optimization targeting only a portion of the circuit, which prevents full design space exploration.

5.1.3 Full Optimization of Two-stage amplifier with 8-bit lock

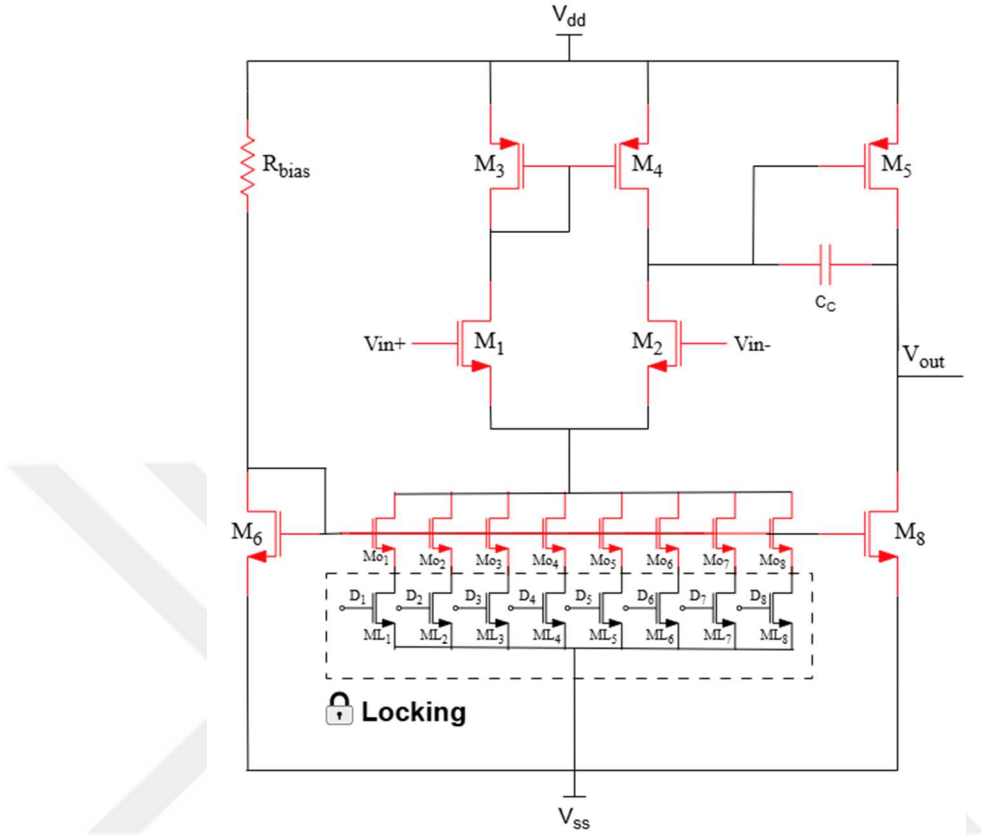


Figure 27: Two-stage amplifier with 8-bit lock. Components shown in red are included in the optimization process.

Full Optimization of the Two-stage Amplifier with an 8-bit lock enables security-aware optimization in a single step. The optimization properties like generation size, swarm size, constraints and objectives are similar to that of *Partial Optimization*; however, in this case, apart from the key transistors, all other transistors are sized by the optimizer as shown in **Figure 27**.

5.1.3.1 Performance optimization

Same cost function which is provided in equation 5.1.2 is used to do performance optimization. The circuit is optimized with the correct key to meet the performance criteria and achieve improved results without considering security aspect. Average performance cost for 600 generation and 1200 generation are given in **Figure 28** and **Figure 29** respectively. Performance of the best members for optimization runs are given in

Table 6

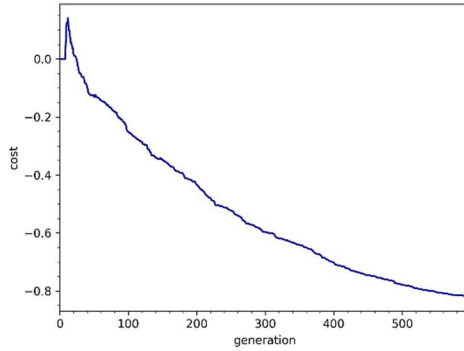


Figure 28: Average Performance Cost of TSO Amplifier with 8-bit Lock (600 generations)

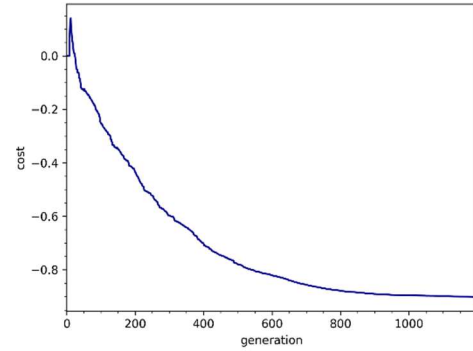


Figure 29: Average Performance Cost of TSO Amplifier with 8-bit Lock (1200 generations)

Table 6: Performance specifications of the best member after 600 and 1200 generations of performance optimization.

Num. of gen.	Convergence Point	Gain	3dB bandwidth	Phase margin	Power	Area
600	596	60.3365dB	29.610k	61.613°	80.14uW	221.8um ²
1200	1176	60.0112dB	29.960k	67.479°	92.61uW	145.3um ²

5.1.3.2 Security evaluation of performance optimization

The selected designs were then subjected to security testing, and the results are shown in **Figure 30** and **Figure 31**. The tests revealed 17 keys for the 600-generation run and 32 keys for the 1200-generation run, highlighting the need for further improvement, particularly in terms of security.

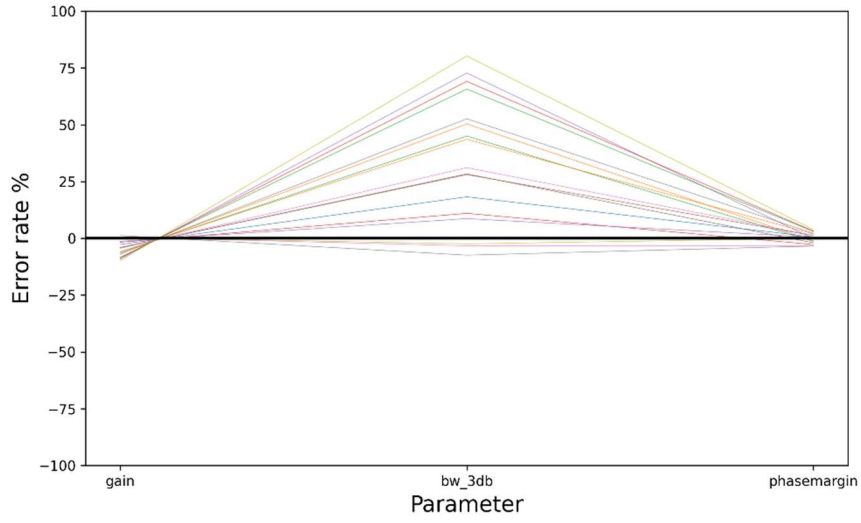


Figure 30: Error rates for each incorrect keys (17) satisfying the threshold after 600 generation.

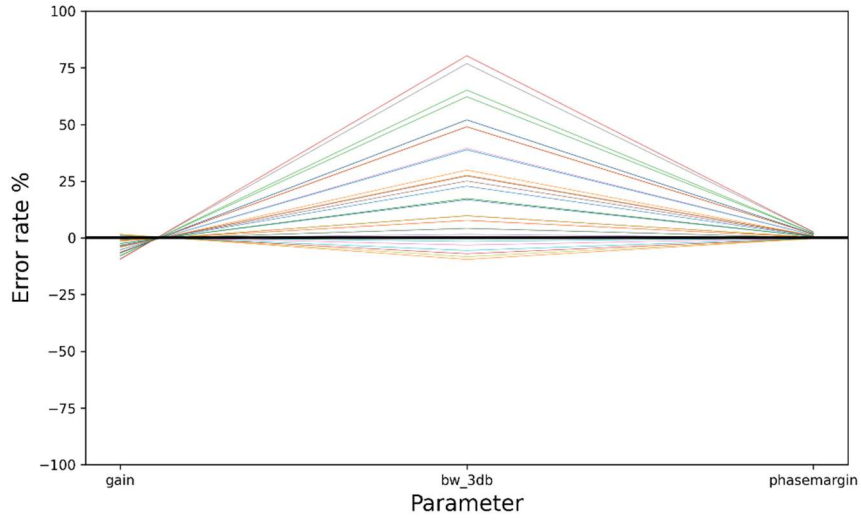


Figure 31: Error rates for each incorrect keys (32) satisfying the threshold after 1200 generation.

5.1.3.3 Performance and security Optimization

For the inclusion of security, the same cost function presented in Section 5.1.3 was applied. Optimization runs were conducted for 600 and 1200 generations, with the resulting average costs shown in **Figure 32** and **Figure 33**. The performance of the best-performing members is summarized in **Table 7**.

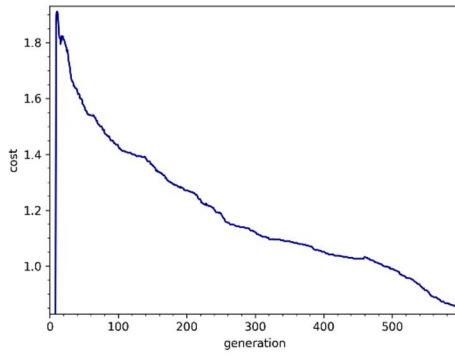


Figure 32: Average Performance + Security Cost of TSO Amplifier with 8-bit Lock (600 generation)

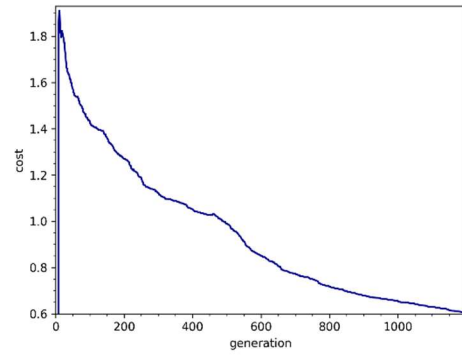


Figure 33: Average Performance + Security Cost of TSO Amplifier with 8-bit Lock (1200 generation)

Table 7: Performance specifications of the best member after 600 and 1200 generations of performance and security optimization.

Num. of gen.	Converge Point	Gain	3dB bandwidth	Phase margin	Power	Area
600	591	65.0079dB	28.450k	50.76°	177.8uW	1164um ²
1200	1191	63.4626dB	29.800k	50.39°	167uW	1088um ²

5.1.3.4 Security evaluation of performance and security optimization

With the inclusion of the security cost in the optimization process, the resulting outcomes are shown in **Figure 34** and **Figure 35**. At 600 generations, the number of keys decreases from 17 to 1, while at 1200 generations it decreases from 32 to 0.

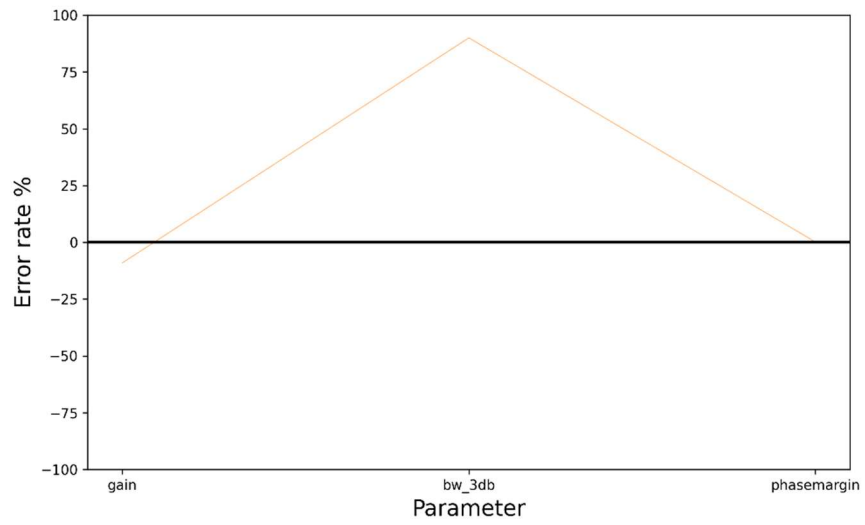


Figure 34: Error rates for each incorrect keys (1) satisfying the threshold after 1200 generation.



Figure 35: Error rates for each incorrect keys (0) satisfying the threshold after 1200 generation.

5.1.4 Summary of Two stage amplifier optimization

Table 8: Summary of Security Results for Two Stage Amplifier.

Optimization type	Cost type	Number of Generation	Convergence Point	Number of acceptable wrong keys	Wrong key pass rate
Partial Optimization	Performance	600	154	56	%21.87
		1200	154	56	%21.87
	Performance + security	600	295	28	%10.93
		1200	295	28	%10.93
Full Optimization	Performance	600	596	17	%6.64
		1200	1176	32	%12.5
	Performance + security	600	591	1	%0.39
		1200	1191	0	%0

The complete security results for Two Stage Amplifier are presented in

Table 8. The results demonstrate that the security-aware cost function effectively reduces the occurrence of incorrect keys that still satisfy performance criteria. In *Partial Optimization*, the limited resizing of transistors prevents the elimination of all incorrectly accepted keys. In contrast, during *Full Optimization*, the incorporation of the security cost function reduces the number of acceptable incorrect keys to one at the 591st generation and to zero at the 1191st generation, demonstrating the effectiveness of the proposed approach.

5.2 Bandgap Reference Circuit

5.2.1 Optimization of Bandgap Reference Circuit (without security)

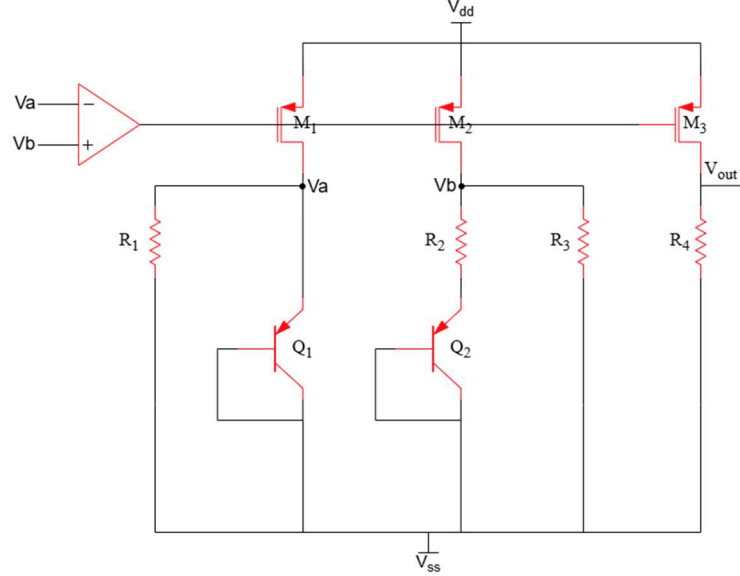


Figure 36: Bandgap Reference Circuit. Components shown in red are included in the optimization process.

As before, to evaluate the potential of the topology and assess the impact of the security elements, optimization was first performed without incorporating any security features. The cost function defined in Equation 5.2.1 was employed, and the same configurations were used for the BGR run, as shown in **Table 2**. Detailed schematic was given in **Figure 36**.

$$Cost = \left[\begin{array}{c} (c_1 P_{norm} + c_2 A_{norm} + c_3 T C_{norm}) - \\ (c_4 PSR_{norm}) \end{array} \right] \quad (5.2.1)$$

$$c_1 = 1, c_2 = 1, c_3 = 1, c_4 = 0.2$$

Objective is to minimize the cost function.

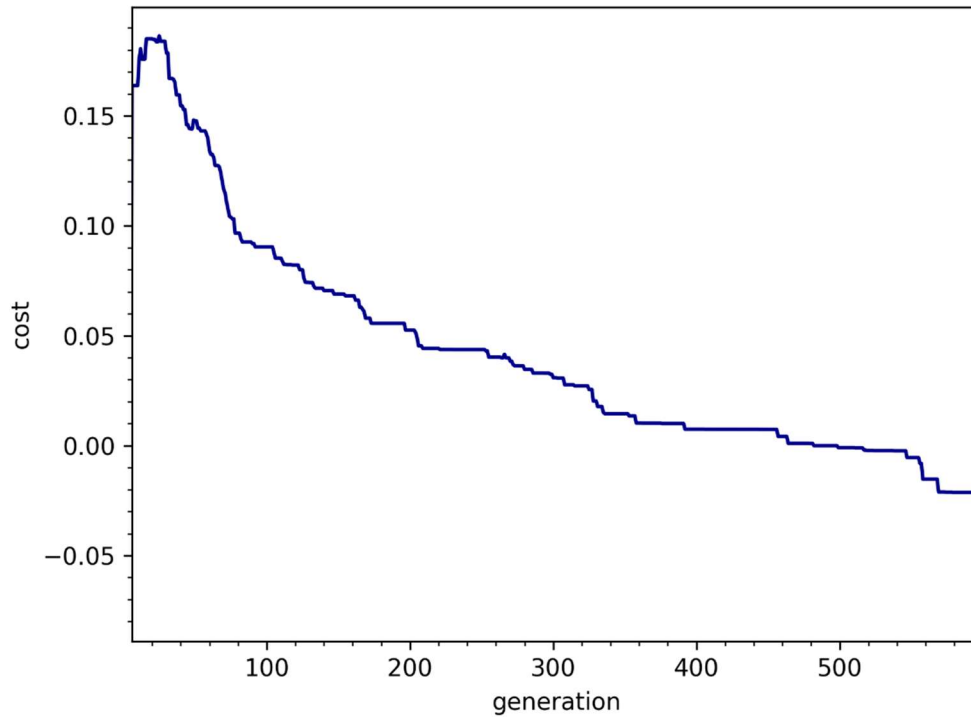


Figure 37: Average Performance Cost of BGR.

Figure 37 shows the average performance cost for the BGR circuit without any security elements. Optimization converged at the 579th generation, out of a maximum of 600 generations. The results, summarized in **Table 9**, demonstrate that the circuit meets the performance requirements.

Table 9: Performance specifications of the best member after 600 generations of performance optimization.

Output Voltage	Convergence Point	Temperature Coefficient (TC)	PSR	Power	Area
0.6929 V	579	10.9044	79.7876°	17.26uW	554.1um ²

5.2.2 Partial Optimization of Bandgap Reference with 8-bit lock

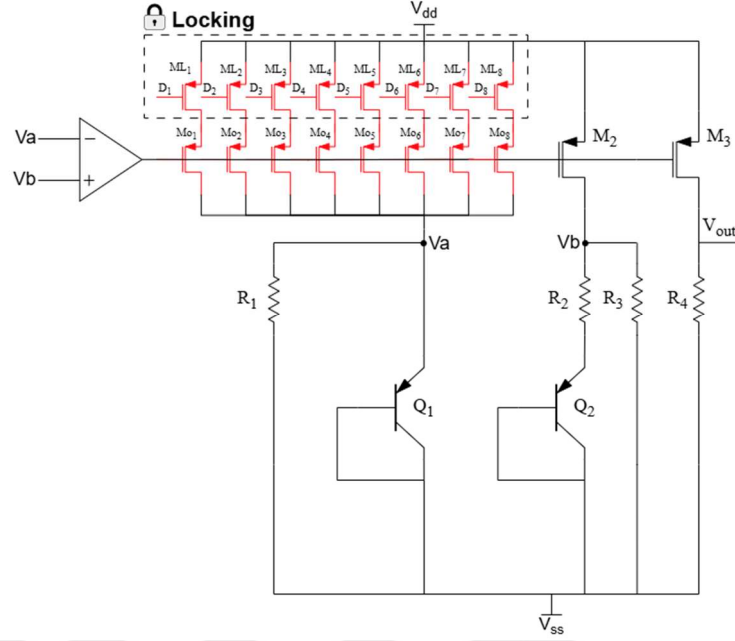


Figure 38: Bandgap Reference Circuit with 8-bit lock. Components shown in red are included in the optimization process.

A combinational 8-bit lock is incorporated into the BGR circuit, as illustrated in **Figure 38**. The current mirror transistor M1 is selected for obfuscation, as the current matching between M1 and M2 is crucial for maintaining the correct output voltage and overall performance of the BGR. Only the locking transistors are targeted during optimization to achieve faster convergence, while the remaining transistors are sized based on the previous optimization run without security. A proper cost function has been formulated to evaluate circuit performance under the correct key entry conditions, as given in Equation 5.2.2.

5.2.2.1 Performance optimization

$$Cost = \left[\frac{(c_1 P_{norm} + c_2 A_{norm} + c_3 TC_{norm})}{(c_4 PSR_{norm})} \right]_{correct_key} \quad (5.2.2)$$

$$c_1 = 1, c_2 = 1, c_3 = 1, c_4 = 0.2$$

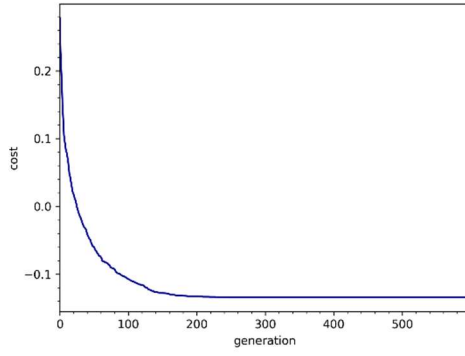


Figure 39: Average Performance Cost of BGR with 8-bit Lock (600 generation)

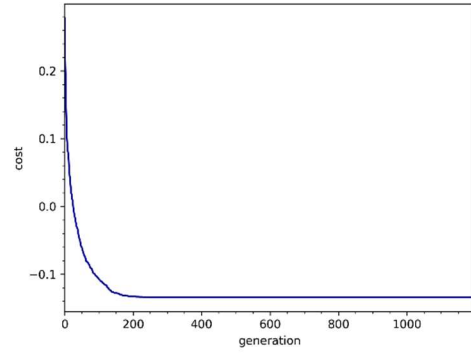


Figure 40: Average Performance Cost of BGR with 8-bit Lock (1200 generation)

Optimization runs with 600 and 1200 iterations were concluded at the 137th generation. The results of these runs are illustrated in **Figure 39** and **Figure 40**, while the resulting performances are summarized in **Table 10**. Both runs yielded identical results that satisfy our performance requirements, with fast convergence.

Table 10: Performance specifications of the best member after 600 and 1200 generations of performance optimization.

Num. of gen.	Convergence Point	Output	TC	PSR	Power	AREA
600	137	0.69 V	21.604	44.4057°	17.17uW	695.6um ²
1200	137	0.69 V	21.604	44.4057°	17.17uW	695.6um ²

5.2.2.2 Security evaluation of performance optimization

After the performance optimization, the security evaluation was conducted, and the combined results are shown in **Figure 41**. The security analysis indicates that 15 incorrect keys still satisfy the performance requirements, highlighting the need to reduce this number.

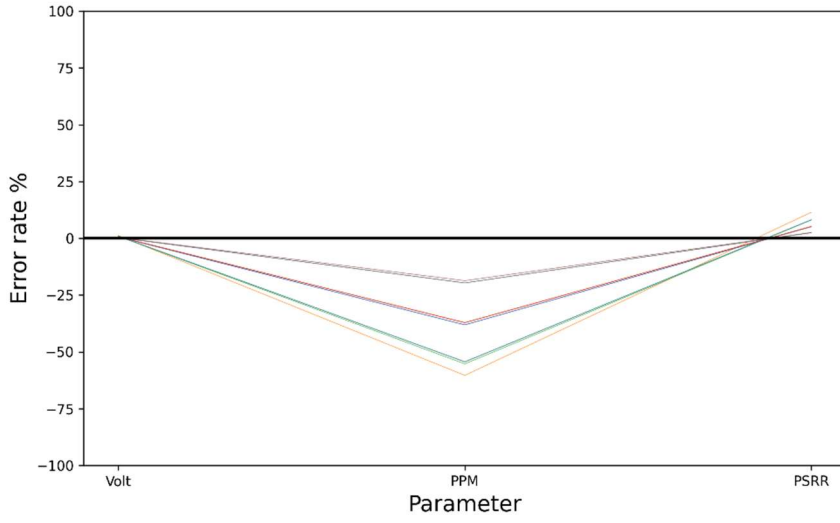


Figure 41: Error rates for each incorrect keys (15) satisfying the threshold after 600 and 1200 generations.

5.2.2.3 Performance and security optimization

To enhance security, the cost function is modified to include a security term, where circuits unlocked with keys having a Hamming distance of one from the correct key are incorporated into the optimization. Performance of the instance that uses those wrong keys will be reduced by optimization while keeping correct circuit in performance requirements.

$$\begin{aligned}
 \text{Performance Cost} &= \left[\frac{(c_1 P_{norm} + c_2 A_{norm} + c_3 TC_{norm})}{(c_4 PSR_{norm})} - \right]_{correct_key} \\
 \text{Security Cost} &= \sum_{n=1}^8 -c_5 \left(TC_{norm_{hamdis_{1n}}} \right) - c_6 \left(OutputVoltage_{norm_{hamdi_{1n}}} \right) \\
 c_1 &= 1, c_2 = 1, c_3 = 1, c_4 = 0.2, c_5 = 0.2, c_6 = 0.6 \\
 \text{Combined Cost function} &= \text{Performance Cost} + \text{Security Cost} \quad (5.2.3)
 \end{aligned}$$

Objective is to minimize the cost function.

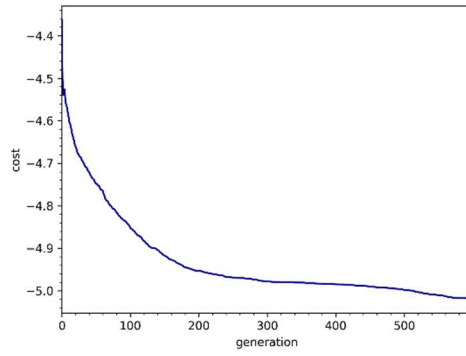


Figure 42: Average Performance + Security Cost of BGR Amplifier with 8-bit Lock (600 generation)

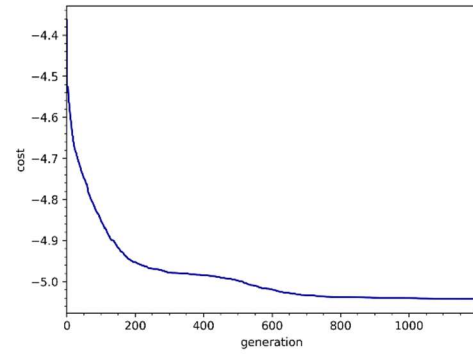


Figure 43: Average Performance + Security Cost of BGR Amplifier with 8-bit Lock (1200 generation)

In **Figure 42** and **Figure 43**, the average cost for performance and security optimization is shown. The resulting performances are listed in **Table 11**. For the 600-generation run, convergence occurs near the end of the run, whereas for the 1200-generation run, it occurs around three-quarters of the way through, indicating that the optimization reaches a good point.

Table 11: Performance specifications of the best member after 600 and 1200 generations of performance and security optimization.

Num. of gen.	Convergence Point	Output	TC	PSR	Power	AREA
600	586	0.6925	24.957	40.9748°	17.28uW	1043um ²
1200	936	0.6906	24.998	40.1223 °	17.18uW	985um ²

5.2.2.4 Security evaluation of performance and security optimization

The security evaluation shows that even though the convergence points differ, both runs performed exceptionally, achieving zero incorrect keys that satisfy the performance requirements. The 600-generation and 1200-generation results can be seen in Figure 44. The longer run further improved area and power consumption.

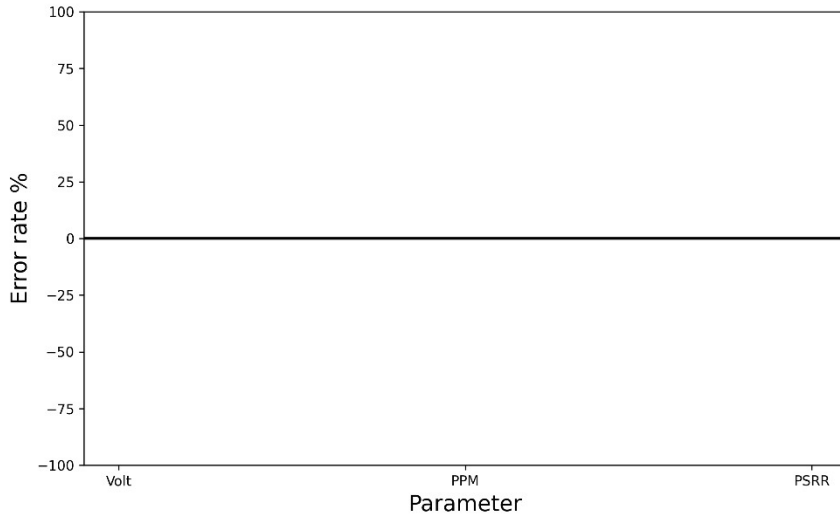


Figure 44: Error rates for each incorrect keys (0) satisfying the threshold after 600 and 1200 generations.

5.2.3 Full Optimization of BGR with 8-bit lock

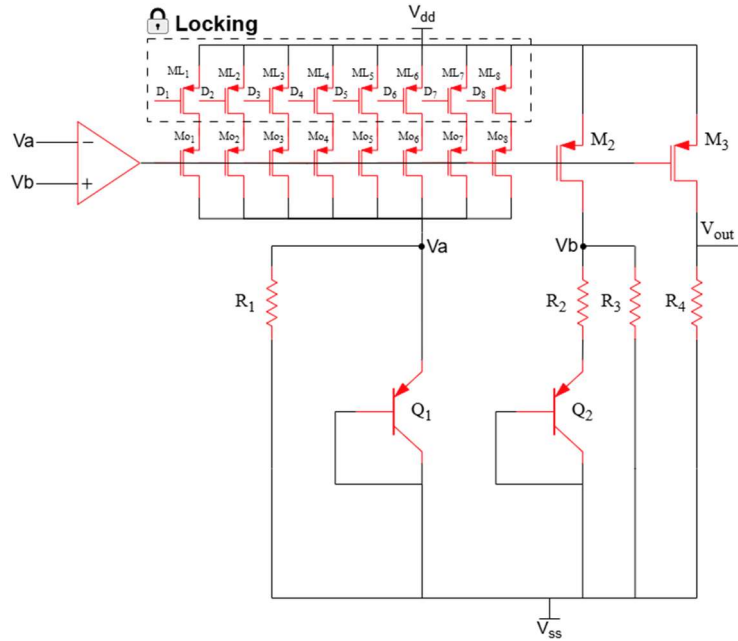


Figure 45: BGR with 8-bit lock. Components shown in red are included in the optimization process.

Full Optimization of the BGR involves optimizing all the transistors and resistors responsible for generating the PTAT and CTAT currents, as well as the operational

amplifier, which is the core element for stabilizing the Va and Vb branches, as illustrated in **Figure 45**. For *Full Optimization*, the same equations and optimization configurations are used as in *Partial Optimization*. The only difference is that with *Full Optimization*, it is possible to create the design in a single run, without performing an initial run to gather sizes for security inclusion.

5.2.3.1 Performance optimization

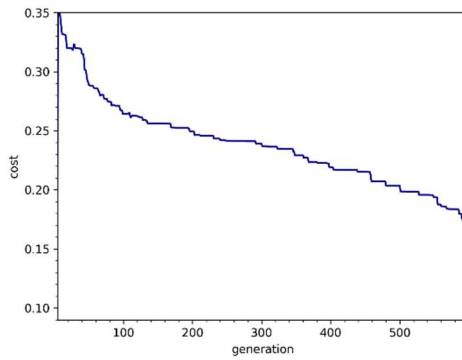


Figure 46: Average Performance Cost of BGR with 8-bit Lock (600 generation)

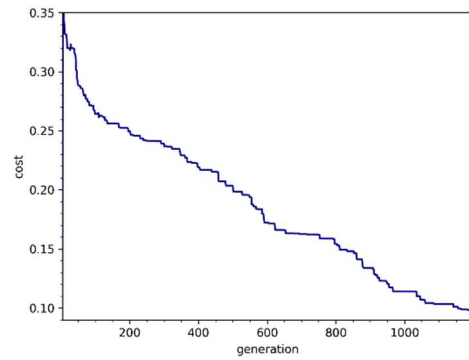


Figure 47: Average Performance Cost of BGR with 8-bit Lock (1200 generation)

When the BGR circuit undergoes performance optimization, the average cost for the 600-generation and 1200-generation runs can be seen in **Figure 46** and **Figure 47**, respectively. The convergence points occur near the end of the optimization, and the resulting performance specifications are given in **Table 12**. The 1200-generation run produced notably improved results.

Table 12: Performance specifications of the best member after 600 and 1200 generations of performance optimization.

Num. of gen.	Convergence Point	Output	TC	PSR	Power	AREA
600	594	0.6906	17.101	45.0741°	16.89uW	1502um ²
1200	1170	0.6901	12.7457	44.8992°	18.15uW	730.2um ²

5.2.3.2 Security evaluation of performance optimization

Even though the correct key performances are satisfactory, security remains insufficient. The 600-generation run has 25 incorrect keys, while the 1200-generation run has 31 incorrect keys, indicating that increased performance for the correct key does not guarantee a secure circuit, as shown in **Figure 48** and **Figure 49**.

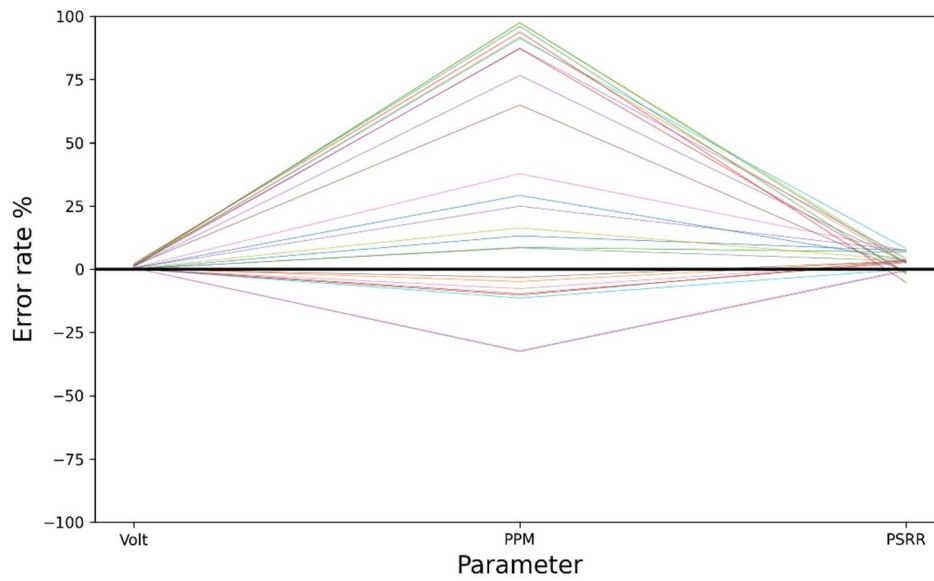


Figure 48: Error rates for each incorrect keys (25) satisfying the threshold after 600 generation.

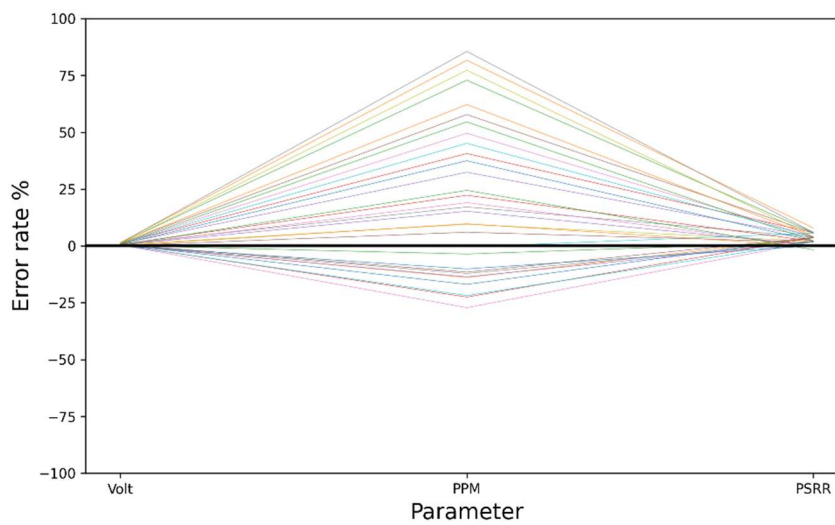


Figure 49: Error rates for each incorrect keys (31) satisfying the threshold after 1200 generation.

5.2.3.3 Performance and security Optimization

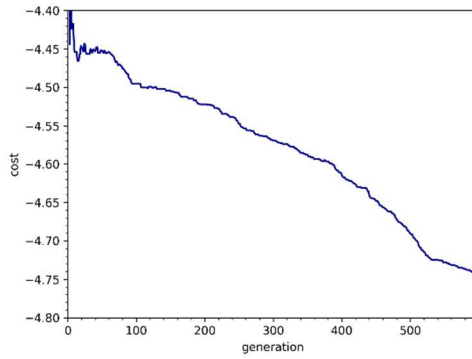


Figure 50: Average Performance + Security Cost of BGR with 8-bit Lock (600 generation)

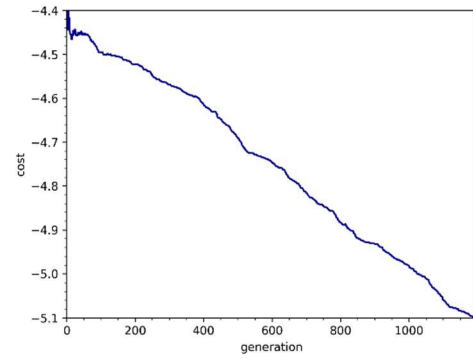


Figure 51: Average Performance + Security Cost of BGR with 8-bit Lock (1200 generation)

For the cost function that includes both performance and security optimization, although the performance remains within the required specifications, there is an increase in area and power consumption. The cost graphs are shown in **Figure 50** and **Figure 51**, and the specifications are listed in **Table 13**.

Table 13: Performance specifications of the best member after 600 and 1200 generations of performance and security optimization.

Num. of gen.	Convergence Point	Output	TC	PSR	Power	AREA
600	586	0.7099	17.7476	42.7046°	19.67uW	1505um ²
1200	1197	0.7076	18.5031	40.2556°	21.31uW	1321um ²

5.2.3.4 Security evaluation of performance and security optimization

Despite the drawback of increased area and power, security performance improves significantly. For the 600-generation run, the number of incorrect keys satisfying the requirements decreases from 25 to 16 shown in **Figure 52**, and for the 1200-generation run, it decreases from 31 to 0 shown in **Figure 53**, demonstrating a substantial improvement.

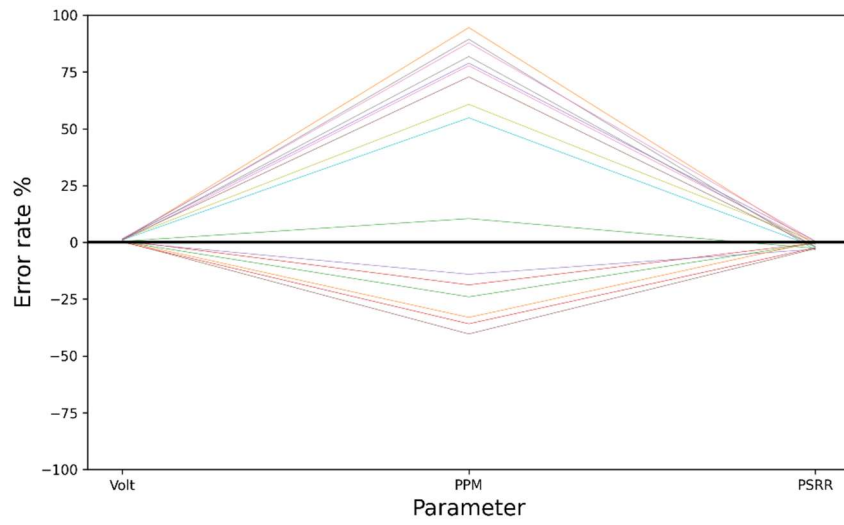


Figure 52: Error rates for each incorrect keys (16) satisfying the threshold after 600 generation.

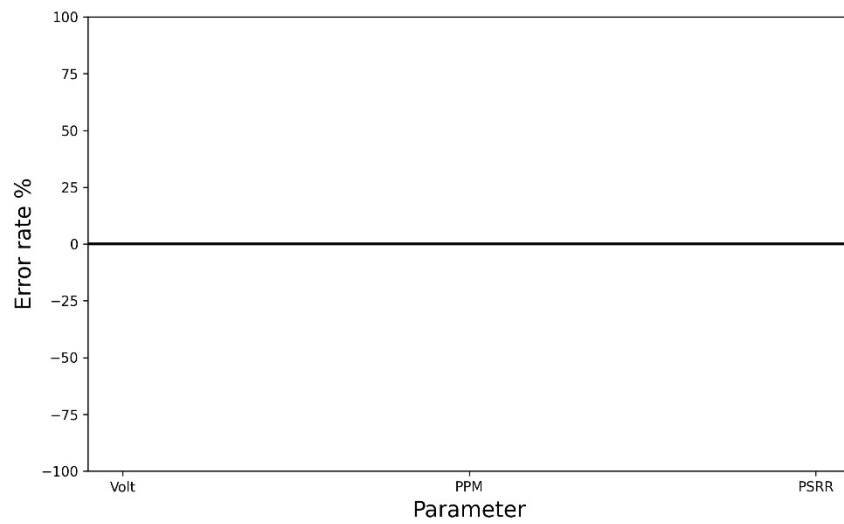


Figure 53: Error rates for each incorrect keys (0) satisfying the threshold after 1200 generation.

5.2.4 Summary of Bandgap Reference Optimization

The complete security results for Bandgap Reference are presented in **Table 14**. The combination of performance and security cost resulted in improved security. For *Partial Optimization*, both runs achieved exceptional security with zero accepted incorrect keys. For *Full Optimization*, the same level of security performance is achieved by the 1197th generation in the 1200-generation run.

Table 14: Summary of Security Results for BGR.

Optimization type	Cost type	Number of Generation	Convergence Point	Number of acceptable wrong keys	Wrong key pass rate
Partial Optimization	Performance	600	137	15	%5.85
		1200	137	15	%5.85
	Performance + security	600	586	0	%0
		1200	936	0	%0
Full Optimization	Performance	600	594	25	%9.76
		1200	1197	31	%12.1
	Performance + security	600	586	16	%6.25
		1200	1197	0	%0

6. CONCLUSION AND FUTURE WORK

The increasing demand for integrated circuit (IC) devices and the rapid advancement of automation have made hardware security a central concern in modern engineering. Across their entire lifecycle—from design to end-of-life—electronic devices are exposed to numerous potential threats, highlighting the necessity of effective and systematic security measures. Untrusted foundries can steal the IP and produce counterfeit ICs or overproduce and distribute for themselves. End-of-life products may be reused on different devices and cause unreliability. Rogue employees and malicious manufacturers may introduce hardware trojans in the production chain. Commercially available or illegally obtained devices may be reverse engineered and learn critical technologies. These threats pose great risks to many different areas. Against IP piracy, locking proves its usefulness for many years in analog and especially digital domain. Preventing hardware trojans is challenging because they are often introduced by rogue employees involved in the IC design process or by malicious foundries responsible for manufacturing the design, both of whom have extensive access to the circuit. Split manufacturing with proper precautions can also help to reduce IP piracy and hardware trojan insertion. For reverse engineering, IC camouflages are useful against reverse engineering approaches, yet power and area overhead must be considered to state that camouflaging is cost effective. Physical unclonable functions are widely used in digital domain but also it is applicable for identification and authentication of analog circuits even though their power consumption needed to be taken into consideration. While digital domain has wider spectrum of defense measures, analog domain still lacks considerable progress in combating IP piracy. The inherent differences between analog and digital circuits have resulted in slower progress within the analog domain. Noting that though counterfeiting is much more common in the analog domain, which in turn also makes digital circuits vulnerable. If the analog parts of digital circuits, like BGRs or oscillators that feed microprocessors are not properly working, most of the operation of digital ICs also will be affected. That being said security of analog circuits is mandatory in terms of establishing hardware security and trust. Another lacking area in the analog domain is the effective utilization of automation tools and methodologies. Again, the complex and nonlinear nature of analog circuits makes the usage of optimization and automation harder. In that case automation of analog circuit design

should be further developed to make it more accessible and widely adoptable. With the increased demand for all IC devices, the unification of the topics of security and automation is mandatory. Automation will surely make the implementation of security methods easier and more widespread. Traditionally, security and optimization in analog circuits have suffered from a lack of awareness. This creates great risk to all kinds of devices and systems. In the last decade, many examples show that security of an electronic device is as important as the quality and performance of it. This work highlights these important topics by establishing a framework with the potential for wider applicability and impact. By taking the necessary steps and raising awareness, it is possible to develop secure, efficient, and practical analog systems with the power of automation.

In this work, we introduced a security-aware optimization framework for analog circuits, focusing on improving resistance against incorrect key acceptance while maintaining performance. Through different configurations, the proposed method demonstrated enhanced security, with circuits evaluated in terms of both performance and security. *Partial Optimization*, involving an initial performance optimization followed by combined security and performance optimization, was shown to effectively improve security in a stepwise manner. Single-step optimization, where all transistors are optimized in a single run, also achieved comparable security improvements. While the primary motivation is to protect intellectual property, the approach is not limited to IP protection and can serve broader security objectives. Additionally, automating security optimization in analog circuits represents a significant advancement, enabling more efficient and systematic protection strategies for future designs. To the best of our knowledge, the proposed method has not been implemented before and constitutes a novel approach that can serve as a foundation for further studies.

REFERENCES

- [1] M. Rostami, F. Koushanfar, and R. Karri, “A Primer on Hardware Security: Models, Methods, and Metrics,” *Proc. IEEE*, vol. 102, no. 8, pp. 1283–1295, Aug. 2014, doi: 10.1109/JPROC.2014.2335155.
- [2] Committee On Armed Services United States Senate, “Inquiry Into Counterfeit Electronic Parts In The Department Of Defense Supply Chain.” May 21, 2012.
- [3] R. S. Chakraborty and S. Bhunia, “HARPOON: An Obfuscation-Based SoC Design Methodology for Hardware Protection,” *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 28, no. 10, pp. 1493–1502, Oct. 2009, doi: 10.1109/TCAD.2009.2028166.
- [4] G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” in *Proceedings of the 44th annual conference on Design automation - DAC '07*, San Diego, California: ACM Press, 2007, p. 9. doi: 10.1145/1278480.1278484.
- [5] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, “Physical Unclonable Functions and Applications: A Tutorial,” *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014, doi: 10.1109/JPROC.2014.2320516.
- [6] J. A. Roy, F. Koushanfar, and I. L. Markov, “Ending Piracy of Integrated Circuits,” *Computer*, vol. 43, no. 10, pp. 30–38, Oct. 2010, doi: 10.1109/MC.2010.284.
- [7] Semiconductor Industry Association, “Winning the Battle Against Counterfeit Semiconductor Products.”
- [8] D. Koblah *et al.*, “A Survey and Perspective on Artificial Intelligence for Security-Aware Electronic Design Automation,” *ACM Trans. Des. Autom. Electron. Syst.*, vol. 28, no. 2, pp. 1–57, Mar. 2023, doi: 10.1145/3563391.
- [9] A. Antonopoulos, C. Kapatsori, and Y. Makris, “Trusted Analog/Mixed-Signal/RF ICs: A Survey and a Perspective,” *IEEE Des. Test*, vol. 34, no. 6, pp. 63–76, Dec. 2017, doi: 10.1109/MDAT.2017.2728366.
- [10] K. Swings, G. Gielen, and W. Sansen, “An intelligent analog IC design system based on manipulation of design equations,” in *IEEE Proceedings of the Custom Integrated Circuits Conference*, Boston, MA, USA: IEEE, 1990, p. 8.6/1-8.6/4. doi: 10.1109/CICC.1990.124691.

- [11] F. El-Turky and E. E. Perry, “BLADES: an artificial intelligence approach to analog circuit design,” *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 8, no. 6, pp. 680–692, Jun. 1989, doi: 10.1109/43.31523.
- [12] B. J. Sheu, A. H. Fung, and Y.-N. Lai, “A knowledge-based approach to analog IC design,” *IEEE Trans. Circuits Syst.*, vol. 35, no. 2, pp. 256–258, Feb. 1988, doi: 10.1109/31.1735.
- [13] T. Matsuba, N. Takai, M. Fukuda, and Y. Kubo, “Inference of Suitable for Required Specification Analog Circuit Topology using Deep Learning,” in *2018 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*, Ishigaki, Okinawa, Japan: IEEE, Nov. 2018, pp. 131–134. doi: 10.1109/ISPACS.2018.8923544.
- [14] R. Martins, N. Lourenco, S. Rodrigues, J. Guilherme, and N. Horta, “AIDA: Automated analog IC design flow from circuit level to layout,” in *2012 International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD)*, Seville, Spain: IEEE, Sep. 2012, pp. 29–32. doi: 10.1109/SMACD.2012.6339409.
- [15] E. Kaya, E. Afacan, and G. Dundar, “An Analog/RF Circuit Synthesis and Design Assistant Tool for Analog IP: DATA-IP,” in *2018 15th International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD)*, Prague, Czech Republic: IEEE, Jul. 2018, pp. 1–9. doi: 10.1109/SMACD.2018.8434906.
- [16] E. Sağlıcan and E. Afacan, “MOEA/D vs. NSGA-II: A Comprehensive Comparison for Multi/Many Objective Analog/RF Circuit Optimization through a Generic Benchmark,” *ACM Trans. Des. Autom. Electron. Syst.*, vol. 29, no. 1, pp. 1–23, Jan. 2024, doi: 10.1145/3626096.
- [17] M. M. Alam *et al.*, “Challenges and Opportunities in Analog and Mixed Signal (AMS) Integrated Circuit (IC) Security,” *J. Hardw. Syst. Secur.*, vol. 2, no. 1, pp. 15–32, Mar. 2018, doi: 10.1007/s41635-017-0024-z.
- [18] R. Torrance and D. James, “The State-of-the-Art in IC Reverse Engineering,” in *Cryptographic Hardware and Embedded Systems - CHES 2009*, vol. 5747, C. Clavier and K. Gaj, Eds., in *Lecture Notes in Computer Science*, vol. 5747, Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 363–381. doi: 10.1007/978-3-642-04138-9_26.
- [19] “Degate project website.” [Online]. Available: <https://www.degate.org/>

- [20] M. M. Tehranipoor, U. Guin, and S. Bhunia, “Invasion of the hardware snatchers,” *IEEE Spectr.*, vol. 54, no. 5, pp. 36–41, May 2017, doi: 10.1109/MSPEC.2017.7906898.
- [21] J. A. Kash, J. C. Tsang, and D. R. Knebel, “Method and apparatus for reverse engineering integrated circuits by monitoring optical emission,” US Patent 6,496,022, Dec. 17, 2002
- [22] P. Subramanyan, N. Tsiskaridze, K. Pasricha, D. Reisman, A. Susnea, and S. Malik, “Reverse Engineering Digital Circuits Using Functional Analysis,” in *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2013*, Grenoble, France: IEEE Conference Publications, 2013, pp. 1277–1280. doi: 10.7873/DATE.2013.264.
- [23] M. Tehranipoor and F. Koushanfar, “A Survey of Hardware Trojan Taxonomy and Detection,” *IEEE Des. Test Comput.*, vol. 27, no. 1, pp. 10–25, Jan. 2010, doi: 10.1109/MDT.2010.7.
- [24] Q. Wang, R. L. Geiger, and D. Chen, “Hardware Trojans embedded in the dynamic operation of analog and mixed-signal circuits,” in *2015 National Aerospace and Electronics Conference (NAECON)*, Dayton, OH, USA: IEEE, Jun. 2015, pp. 155–158. doi: 10.1109/NAECON.2015.7443059.
- [25] I. Polian, “Security aspects of analog and mixed-signal circuits,” in *2016 IEEE 21st International Mixed-Signal Testing Workshop (IMSTW)*, Sant Feliu de Guixols, Spain: IEEE, Jul. 2016, pp. 1–6. doi: 10.1109/IMS3TW.2016.7524239.
- [26] G. Goos, J. Hartmanis, J. Van Leeuwen, P. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis,” in *Advances in Cryptology — CRYPTO’ 99*, vol. 1666, M. Wiener, Ed., in Lecture Notes in Computer Science, vol. 1666. , Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 388–397. doi: 10.1007/3-540-48405-1_25.
- [27] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, “The EM Side—Channel(s),” in *Cryptographic Hardware and Embedded Systems - CHES 2002*, vol. 2523, B. S. Kaliski, Ç. K. Koç, and C. Paar, Eds., in Lecture Notes in Computer Science, vol. 2523. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 29–45. doi: 10.1007/3-540-36400-5_4.
- [28] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, “Security analysis of integrated circuit camouflaging,” in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security - CCS ’13*, Berlin, Germany: ACM Press, 2013, pp. 709–720. doi: 10.1145/2508859.2516656.

- [29] L. W. Chow, J. P. Baukus, B. J. Wang, and R. P. Cocchi, “Camouflaging a standard cell based integrated circuit,” Apr. 03, 2012
- [30] R. P. Cocchi, J. P. Baukus, B. J. Wang, L. W. Chow, and P. Ouyang, “Building block for a secure CMOS logic cell library,” US Patent 8,111,089, Feb. 07, 2012
- [31] A. A.- Saki and S. Ghosh, “How Multi-Threshold Designs Can Protect Analog IPs,” in *2018 IEEE 36th International Conference on Computer Design (ICCD)*, Orlando, FL, USA: IEEE, Oct. 2018, pp. 464–471. doi: 10.1109/ICCD.2018.00075.
- [32] J. Leonhard, A. Sayed, M.-M. Louerat, H. Aboushady, and H.-G. Stratigopoulos, “Analog and Mixed-Signal IC Security via Sizing Camouflaging,” *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 40, no. 5, pp. 822–835, May 2021, doi: 10.1109/TCAD.2020.3011662.
- [33] R. W. Jarvis and M. G. McIntyre, “Split manufacturing method for advanced semiconductor circuits,” US Patent 7,195,931, Mar. 27, 2007
- [34] J. (Jv) Rajendran, O. Sinanoglu, and R. Karri, “Is Split Manufacturing Secure?,” in *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2013*, Grenoble, France: IEEE Conference Publications, 2013, pp. 1259–1264. doi: 10.7873/DATE.2013.261.
- [35] Y. Bi, J. Yuan, and Y. Jin, “Beyond the Interconnections: Split Manufacturing in RF Designs,” *Electronics*, vol. 4, no. 3, pp. 541–564, Aug. 2015, doi: 10.3390/electronics4030541.
- [36] K. Vaidyanathan, B. P. Das, E. Sumbul, R. Liu, and L. Pileggi, “Building trusted ICs using split fabrication,” in *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, Arlington, VA, USA: IEEE, May 2014, pp. 1–6. doi: 10.1109/HST.2014.6855559.
- [37] A. B. Kahng *et al.*, “Watermarking techniques for intellectual property protection,” in *Proceedings of the 35th annual conference on Design automation conference - DAC '98*, San Francisco, California, United States: ACM Press, 1998, pp. 776–781. doi: 10.1145/277044.277240.
- [38] N. Narayan, R. D. Newbould, J. D. Carothers, J. J. Rodriguez, and W. T. Holman, “IP protection for VLSI designs via watermarking of routes,” in *Proceedings 14th Annual IEEE International ASIC/SOC Conference (IEEE Cat. No.01TH8558)*, Arlington, VA, USA: IEEE, 2001, pp. 406–410. doi: 10.1109/ASIC.2001.954736.
- [39] U. Das, M. R. Muttaki, M. M. Tehranipoor, and F. Farahmandi, “ADWIL: A Zero-Overhead Analog Device Watermarking Using Inherent IP Features,” in *2022*

IEEE International Test Conference (ITC), Anaheim, CA, USA: IEEE, Sep. 2022, pp. 155–164. doi: 10.1109/ITC50671.2022.00023.

[40] A. Sanabria-Borbon, N. G. Jayasankaran, J. Hu, J. Rajendran, and E. Sanchez-Sinencio, “Analog/RF IP Protection: Attack Models, Defense Techniques, and Challenges,” *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 68, no. 1, pp. 36–41, Jan. 2021, doi: 10.1109/TCSII.2020.3040725.

[41] J. Wang, C. Shi, A. Sanabria-Borbon, E. Sanchez-Sinencio, and J. Hu, “Thwarting analog IC piracy via combinational locking,” in *2017 IEEE International Test Conference (ITC)*, Fort Worth, TX: IEEE, Oct. 2017, pp. 1–10. doi: 10.1109/TEST.2017.8242064.

[42] V. Venugopal Rao and I. Savidis, “Performance and Security Analysis of Parameter-Obfuscated Analog Circuits,” *IEEE Trans. Very Large Scale Integr. VLSI Syst.*, vol. 29, no. 12, pp. 2013–2026, Dec. 2021, doi: 10.1109/TVLSI.2021.3109062.

[43] G. Volanis, Y. Lu, S. G. Rao Nimmalapudi, A. Antonopoulos, A. Marshall, and Y. Makris, “Analog Performance Locking through Neural Network-Based Biasing,” in *2019 IEEE 37th VLSI Test Symposium (VTS)*, Monterey, CA, USA: IEEE, Apr. 2019, pp. 1–6. doi: 10.1109/VTS.2019.8758657.

[44] M. Elshamy, A. Sayed, M.-M. Louerat, A. Rhouni, H. Aboushady, and H.-G. Stratigopoulos, “Securing Programmable Analog ICs Against Piracy,” in *2020 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Grenoble, France: IEEE, Mar. 2020, pp. 61–66. doi: 10.23919/DATE48585.2020.9116520.

[45] V. V. Rao and I. Savidis, “Protecting analog circuits with parameter biasing obfuscation,” in *2017 18th IEEE Latin American Test Symposium (LATS)*, Bogota, Colombia: IEEE, Mar. 2017, pp. 1–6. doi: 10.1109/LATW.2017.7906739.

[46] N. G. Jayasankaran, A. S. Borbon, E. Sanchez-Sinencio, J. Hu, and J. Rajendran, “Towards provably-secure analog and mixed-signal locking against overproduction,” in *Proceedings of the International Conference on Computer-Aided Design*, San Diego California: ACM, Nov. 2018, pp. 1–8. doi: 10.1145/3240765.3240858.

[47] A. R. D. Rizo, J. Leonhard, H. Aboushady, and H.-G. Stratigopoulos, “RF Transceiver Security Against Piracy Attacks,” *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 69, no. 7, pp. 3169–3173, Jul. 2022, doi: 10.1109/TCSII.2022.3165709.

[48] “Static Physically Unclonable Functions for Secure Chip Identification With 1.9–5.8% Native Bit Instability at 0.6–1 V and 15 fJ/bit in 65 nm,” *IEEE J. Solid-State Circuits*, vol. 51, no. 3, pp. 763–775, Mar. 2016, doi: 10.1109/JSSC.2015.2506641.

- [49] J. Li and M. Seok, "Ultra-Compact and Robust Physically Unclonable Function Based on Voltage-Compensated Proportional-to-Absolute-Temperature Voltage Generators," *IEEE J. Solid-State Circuits*, vol. 51, no. 9, pp. 2192–2202, Sep. 2016, doi: 10.1109/JSSC.2016.2586498.
- [50] M. Majzoobi, G. Ghiaasi, F. Koushanfar, and S. R. Nassif, "Ultra-low power current-based PUF," in *2011 IEEE International Symposium of Circuits and Systems (ISCAS)*, Rio de Janeiro, Brazil: IEEE, May 2011, pp. 2071–2074. doi: 10.1109/ISCAS.2011.5938005.
- [51] J. Kennedy and R. Eberhart, "Particle swarm optimization," in *Proceedings of ICNN'95 - International Conference on Neural Networks*, Perth, WA, Australia: IEEE, 1995, pp. 1942–1948. doi: 10.1109/ICNN.1995.488968.
- [52] Zhi-Hui Zhan, Jun Zhang, Yun Li, and H. S.-H. Chung, "Adaptive Particle Swarm Optimization," *IEEE Trans. Syst. Man Cybern. Part B Cybern.*, vol. 39, no. 6, pp. 1362–1381, Dec. 2009, doi: 10.1109/TSMCB.2009.2015956.
- [53] J. Blank and K. Deb, "Pymoo: Multi-Objective Optimization in Python," *IEEE Access*, vol. 8, pp. 89497–89509, 2020, doi: 10.1109/ACCESS.2020.2990567.

BIOGRAPHY

Abdullah Bayram graduated from Sakıp Sabancı Anatolian High School in 2017. He earned his bachelor's degree in electrical engineering from Gebze Technical University in 2022. He is currently pursuing his master's degree at Gebze Technical University.



PUBLICATIONS AND PRESENTATIONS FROM THE THESIS

A. Bayram, E. Sağlıcan and E. Afacan, "Performance Optimization After Hardware Security in Analog Integrated Circuits," 2024 15th National Conference on Electrical and Electronics Engineering (ELECO), Bursa, Türkiye, 2024, pp. 1-5

