ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL

# MAZE-BASED SHIELD DESIGN TO PROTECT ICs AGAINST INVASIVE HARDWARE ATTACKS

**M.Sc. THESIS**

**Raşit Rıdvan TURGUT**

**Department of Electronics and Communication Engineering**

**Electronics Engineering Programme**

**FEBRUARY 2024**

**ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL**

# MAZE-BASED SHIELD DESIGN TO PROTECT ICs AGAINST INVASIVE HARDWARE ATTACKS

**M.Sc. THESIS**

**Raşit Rıdvan TURGUT**
**(504201229)**

**Department of Electronics and Communication Engineering**

**Electronics Engineering Programme**

**Thesis Advisor: Prof. Dr. Müştak Erhan YALÇIN**

**FEBRUARY 2024**

**İSTANBUL TEKNİK ÜNİVERSİTESİ ★ LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ**

# İSTİLACİ DONANIM SALDIRILARINA KARŞI ENTEGRE DEVRELERİ KORUMAK İÇİN LABİRENT TABANLI KALKAN TASARIMI

**YÜKSEK LİSANS TEZİ**

**Raşit Rıdvan TURGUT**
**(504201229)**

**Elektronik ve Haberleşme Mühendisliği Anabilim Dalı**

**Elektronik Mühendisliği Programı**

**Tez Danışmanı: Prof. Dr. Müştak Erhan YALÇIN**

**ŞUBAT 2024**

Raşit Rıdvan TURGUT, a M.Sc. student of ITU Graduate School student ID 504201229 successfully defended the thesis entitled "MAZE-BASED SHIELD DESIGN TO PROTECT ICs AGAINST INVASIVE HARDWARE ATTACKS", which he/she prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

| | | |
|---|---|---|
| **Thesis Advisor :** | **Prof. Dr. Müştak Erhan YALÇIN**<br>Istanbul Technical University | ..... |
| **Jury Members :** | **Asst. Prof. Dr. Faik BAŞKAYA**<br>Boğaziçi University | ..... |
| | **Prof. Dr. Mustafa ALTUN**<br>Istanbul Technical University | ..... |
| | | ..... |

**Date of Submission :** **5 January 2024**
**Date of Defense :** **21 February 2024**

## FOREWORD

Foremost, I would like to thank Prof. Dr. Müştak Erhan YALÇIN, Can KURT, and Asst. Prof. Dr. Faik BAŞKAYA for all their support and guidance during my M.Sc. thesis.

I would also like to express my gratitude to my family for their continuous support through all of my life.

A part of this work has been realized within the framework of the TUBITAK research project 5210073.

February 2024 Raşit Rıdvan TURGUT

**TABLE OF CONTENTS**


| | Page |
|---|---|
| **FOREWORD** | **vii** |
| **TABLE OF CONTENTS** | **ix** |
| **ABBREVIATIONS** | **xi** |
| **LIST OF TABLES** | **xiii** |
| **LIST OF FIGURES** | **xv** |
| **SUMMARY** | **xvii** |
| **ÖZET** | **xix** |
| **1. INTRODUCTION** | **1** |
| 1.1 Literature Review | 2 |
| 1.2 Hypothesis | 3 |
| **2. BACKGROUND** | **5** |
| 2.1 Hardware Attacks | 5 |
| 2.1.1 Non-invasive attacks | 6 |
| 2.1.2 Invasive attacks | 6 |
| 2.1.3 Decapsulation | 6 |
| 2.1.4 Microprobing | 7 |
| 2.1.5 Focused ion beam (FIB) | 8 |
| 2.2 Active Shield Protection for Hardware Attacks | 10 |
| 2.2.1 Active shield architecture | 11 |
| 2.2.2 Shield structure requirements | 12 |
| 2.2.2.1 Complexity | 12 |
| 2.2.2.2 Connectivity and full coverage | 13 |
| 2.3 Multi-Layer Shield Technique | 15 |
| **3. GENERATION OF MAZE SHIELD TO ACTIVE PROTECTION AGAINST HARDWARE ATTACKS** | **17** |
| 3.1 Maze Based Shield | 17 |
| 3.1.1 Usage of maze algorithms for maze shield generation | 18 |
| 3.1.2 Generation of maze shield | 22 |
| **4. MULTI LAYER RANDOM MAZE SHIELD GENERATION AND VERIFICATION** | **27** |
| 4.1 Generation of Multi-Layer Shield | 27 |
| 4.2 Generation of Multi-Layer Shield Using Small Multi-Layer Shields | 31 |
| **5. CONCLUSIONS** | **33** |
| **REFERENCES** | **35** |
| **CURRICULUM VITAE** | **37** |

**ABBREVIATIONS**

**IC** **:** Integrated Circuit
**VIA** **:** Vertical Interconnect Access
**FIB** **:** Focused Ion Beam

## LIST OF TABLES

**Page**

**Table 3.1 :** Entropy Results of Maze-Shield ..... **22**

## LIST OF FIGURES


**Page**

**Figure 1.1 :** IC Market Size, 2022 to 2032(USD BILLION) [1] ..... **1**
**Figure 2.1 :** Milling a cavity into the desoldered chip [2] ..... **7**
**Figure 2.2 :** Chip decapsulation with nitric acid (left), rinsing with acetone (right). [2] ..... **7**
**Figure 2.3 :** Probing Attacks [3] ..... **8**
**Figure 2.4 :** (a) FIB deposits platinum in the milling cavity to build conducting the path from the target wire. (b) The deposited conducting path serves as an electrical probe contact. [4] ..... **9**
**Figure 2.5 :** Unlock the access to an internal memory thanks to FIB [3] ..... **10**
**Figure 2.6 :** Active Shield Architecture ..... **11**
**Figure 2.7 :** Re-Routing Attack ..... **13**
**Figure 2.8 :** Hamiltonian Cycles [5] ..... **14**
**Figure 2.9 :** FIB Attacks with different aspect ratio on Multi-Layer Shield [4] ... **16**
**Figure 3.1 :** Single Layer Maze-Shield with using AFSA ..... **20**
**Figure 3.2 :** Single Layer Maze-Shield with using MST ..... **21**
**Figure 3.3 :** The Foreground Generation Part of Picturesque Technique [6] ..... **23**
**Figure 3.4 :** Shield Generation with Using Maze Algorithm Output ..... **24**
**Figure 3.5 :** Generated Maze and Generated Shield ..... **25**
**Figure 4.1 :** Multi-Layer Shields Generated with Identical Single-Layer Shields **29**
**Figure 4.2 :** Forming Undesired Loop during Layers Connection Operation ..... **30**
**Figure 4.3 :** The Shield Structure Generated with Four Small Shields ..... **31**
**Figure 5.1 :** The Shield Structure into Digital Design Flow ..... **34**

**MAZE-BASED SHIELD DESIGN**
**TO PROTECT ICs AGAINST INVASIVE HARDWARE ATTACKS**

## SUMMARY

Integrated Circuit (IC) technology has gained significant importance today and found a wide range of applications. However, hardware attacks pose a potential threat by enabling unauthorized access to sensitive data within the system, which is a prominent concern for users and the industry.

Hardware attacks aimed at accessing critical data in IC architectures can be categorized into non-invasive and invasive attacks. Non-invasive attacks involve analyzing side-channel information or software-based interventions, while invasive attacks require physical access to the circuit's internal structure. Non-invasive attacks include Interference, Fault Injection, Electromagnetic, and Optical Fault Injection. Invasive attacks include Chip Decapsulation, Microprobe Usage, and Focused Ion Beam Attack. These attacks reveal security vulnerabilities in IC architectures and highlight the need for improved security measures.

This thesis proposes a maze-based shield structure to enhance the security of ICs against invasive hardware attacks, which require physical access. The maze-based multi-layered shield structure is designed to protect confidential data within ICs from invasive hardware attacks. It provides active shield protection by monitoring the flow of a bit sequence through the shield. Building a shield that works well must have three key features: complexity, connectivity, and full coverage. A maze-based structure provides the necessary complexity, while connectivity ensures data flows smoothly through the shield. Full coverage means that the shield must cover all the points in a graph. When a shield satisfies the Hamiltonian cycle condition, it is fully covered and connected.

Maze algorithms can create intricate patterns but do not inherently have the Hamiltonian cycle property. To fulfill this condition, the shield generation algorithm uses the maze algorithm's outputs and establishes connections between each new node. In the thesis, the "Minimum Spanning Tree (MST)" and "Artificial Fish Swarm Algorithm (AFSA)" are used for maze production. The entropy of the directions in the generated shield structures is used as a complexity metric.

This thesis discusses the creation of multi-layered shields for IC security. Single-layer shields are becoming less reliable due to evolving hardware attack methods. The multi-layered shield structure provides more effective protection. It involves connecting two single-layer shield structures with common paths to create a maze-based multi-layered shield structure that meets complexity and Hamiltonian cycle requirements. However, undesired loop structures may form, leading to the violation of the Hamiltonian cycle condition. A loop control algorithm has been developed and added to the production stage to prevent this.

A multi-layer shield generation using a small multi-layer shields algorithm has been designed to produce shields for protecting larger areas. This algorithm divides the area into N horizontal and M vertical areas and runs the maze-based multi-layered shield structure creation algorithm N x M times. The resulting shield structure provides a more robust defense against hardware attacks, protecting sensitive data within IC structures.

As a future task, covering a large area with multiple shield structures and creating interleaved sub-shields structures can be added to achieve more effective protection by transforming the algorithm structure designed within this thesis's scope.

# İSTİLACİ DONANIM SALDIRILARINA KARŞI ENTEGRE DEVRELERİ KORUMAK İÇİN LABİRENT TABANLI KALKAN TASARIMI

## ÖZET

Gelişen Entegre Devre teknolojisinin hızla ilerlemesiyle birlikte, günümüzde Entegre Devre yapıları, teknolojik sistemler içerisinde kilit bir konuma ve büyük bir öneme sahiptir. Bu yapılar, çeşitli sektörlerde geniş bir uygulama yelpazesi bulmuş ve birçok farklı alanda kullanılmaktadır. Ancak, bu geniş kullanım alanlarına paralel olarak, Entegre Devre yapıları içerisinde depolanan kritik bilgilerin güvenliği de öne çıkan bir sorun haline gelmiştir.

Günümüzde, Entegre Devreler üzerinde gerçekleştirilebilen donanım saldırıları, sistemin içerisinde barındırdığı hassas verilere yetkisiz erişim sağlama potansiyeli taşımaktadır. Bu durum, kullanıcılar ve endüstri açısından istenmeyen bir güvenlik tehdidi oluşturmaktadır.

Entegre Devre yapıları içindeki kritik verilere ulaşma amacı güden saldırganlar, donanımsal saldırı tekniklerine başvurmaktadır. Bu teknikler, genellikle iki ana kategoride incelenebilir: istilacı olmayan ve istilacı donanımsal saldırılar. İstilacı olmayan donanımsal saldırılar, genellikle fiziksel erişim gerektirmeyen yöntemleri kapsar ve yan kanal bilgilerinin analizi veya yazılım temelli müdahaleleri içerir. Yan kanal saldırıları, Girişim Saldırıları, Hata Enjeksiyon Saldırıları, Elektromanyetik Hata Enjeksiyonu ve Optik Hata Enjeksiyonu gibi alt kategorilere ayrılır. Yan kanal saldırıları, cihazın yan kanal bilgilerini analiz ederek, güç tüketimi, elektromanyetik radyasyon veya zamanlama gibi yan kanal bilgilerini kullanarak hassas bilgileri çıkarma amacını taşır. Girişim saldırıları, cihazın normal işleyişini bozmak için enerji dalgalanmalarını hedefler. Hata enjeksiyon saldırıları, sisteme kasıtlı olarak hatalar enjekte ederek normal işleyişi bozmaya çalışır. Elektromanyetik hata enjeksiyonu, elektromanyetik alanlar kullanarak hedef sistemi hedef alırken, optik hata enjeksiyonu ise lazer veya ışık kaynakları kullanarak optik yollarla hatalar enjekte etmeyi içerir. Öte yandan, istilacı donanımsal saldırılar, genellikle fiziksel erişimi gerektiren ve entegre devrenin iç yapısına yönelik müdahaleleri içeren saldırı türlerini içerir. Bu tür saldırılarda saldırganlar, genellikle entegre devrenin dış kapsülünü açarak veya mikroskobik iğneler kullanarak devrenin iç bileşenlerine erişim sağlarlar. Çip Kapsülünün Açılması, Mikroprobe Kullanma ve Odaklı İyon Demeti Saldırısı gibi alt kategoriler, istilacı donanımsal saldırı türlerini temsil eder. Çip kapsülünün açılması, entegre devrenin dış kapsülünü açarak iç yapısına erişmeyi amaçlar. Mikroprobe kullanma, mikroskobik iğneler kullanarak devrenin iç bileşenleriyle etkileşime geçilmesine odaklanır. Odaklı iyon demeti saldırısı ise iyon demeti odaklı bir demet kullanarak devreye müdahale eder ve iç yapısında değişiklikler yapmayı hedefler. Bu donanımsal saldırı teknikleri, entegre devre yapılarındaki güvenlik açıklarını vurgulayarak, bu alandaki güvenlik önlemlerinin geliştirilmesi konusunda önemli bir odak noktası oluşturmaktadır.

İstilacı olmayan saldırılara karşı alınabilecek önlemler genellikle, yan kanal bilgilerinin analiz edilmesini zorlaştıracak, güç tüketimi, elektromanyetik radyasyon veya zamanlama gibi yan kanal bilgilerini koruyacak ve bu tür saldırıları önleyecek güçlü şifreleme yöntemlerinin uygulanmasını içermektedir. Buna karşın, istilacı donanımsal saldırılara karşı alınabilecek önlemler, fiziksel erişim gerektiren doğası nedeniyle daha zor ve karmaşık olabilir. Bu tez, söz konusu güvenlik zorluğuna etkili bir çözüm sunmak amacıyla çok katmanlı labirent tabanlı bir kalkan yapısı önermektedir. Labirent tabanlı kalkan yapısı, entegre devrelerin güvenliğini artırmak ve istilacı donanım saldırılarına karşı bir çözüm sunmaktadır.

Labirent tabanlı çok katmanlı kalkan yapısı Entegre Devreler içerisindeki gizli verilerin istilacı donanım saldırılarından korunması hedeflemektedir. Labirent tabanlı çok katmanlı kalkan yapısının Entegre Devre üzerinde aktif kalkan koruması sağlaması hedeflenmektedir. Aktif kalkan koruması, dijital bir devre ile üretilmiş bit dizisinin kullanılan kalkan üzerinden kesintisiz bir şekilde aktığını kontrol etmeye dayalı koruma yöntemidir. Dijital ortamda bulunan bit kontrol devresi sayesinde girişten gönderilen bit bilgisinin tüm kalkan üzerinden aktığını yani kalkan üzerinde bağlantısal bir sorun olmadığını garanti etmeye dayanır. Kalkan üzerinde herhangi bir bağlantı problemi olduğu tespit edilirse donanımsal bir saldırı olduğu tespit edilmiş olur. Bu sayede Entegre Devre içerisindeki kritik verilerin korunması sağlanmış olur.

Bu amaçla oluşturulmuş yapının korunması istenilen bölgeleri etkin bir şekilde koruyabilmesi için bazı özelliklere sahip olması gerekmektedir. Bu özelliklerden ilki karmaşık bir yapıya sahip olmasıdır. İstilacı donanım saldırılarında, saldırganlar Entegre Devrelerin iç yapılarını analiz etmektedir. Bu analizler sonucunda devrenin yapısını çözüp kritik verileri elde etmeyi hedeflemektedirler. Karmaşık bir kalkan yapısıyla gizli verilerin saklandığı alanların kapatılması yöntemiyle saldırganların bu verileri elde etmesi engellenebilir. Labirent yapıları karmaşıklık üzerine kurgulanmış yapılardır. Labirent tabanlı kalkan üretimi bu gereksinimi karşılamak amaçlı kullanılmıştır. Kalkan yapısının diğer temel özelliği bağlanırlık. Bağlanırlık özelliği kalkan yapısının dijital bir devre tarafından üretilmiş bit dizisinin kalkan üzerinden geçerek bit kontrol devresine ulaşmasını sağlayacak özelliktir. Bu özellik sayesinde kalkan üzerinden akan bit dizisinin kontrolü yapılıp aktif koruma devresi sağlanmış olacaktır. Etkili bir kalkan yapısının son özelliği de tam kapsayıcılıktır. Tam kapsayıcılık, kalkan tarafından korunması istenilen alandaki tüm düğümlerin kalkan yapısına dahil olmasını ifade eder. Bu sayede kalkan ile korunmak istenilen alanda herhangi bir boşluk kalmayarak saldırgan için potansiyel bir saldırı noktası bırakılmamış olur. Hamiltonian çemberi özelliğine sahip bir kalkan yapısı bağlanırlık ve tam kapsayacılık özelliklerini sağlayan bir yapı oluşturacaktır. Hamiltonian çember, bir grafın tüm düğümlerini içeren ve başlangıç düğümüne geri dönen bir çevreyi ifade eder. Yani, bir grafın Hamiltonian çemberi, başlangıç düğümünden başlayarak her düğümü yalnızca bir kez ziyaret eden bir çemberdir. Bu tez kapsamında bağlanırlık ve tam kapsayılılık özellikleri birleştirilerek Hamiltonian çemberi koşulu olarak isimlendirilmiştir.

Aktif kalkan yapısının temel gereksinimlerden biri olan karmaşık bir yapıya sahip olması özelliği labirent algoritmaları ile sağlanabilmektedir. Labirent algoritmaları tabiatı gereği karmaşık bir görüntü örüntüsü oluşturmayı hedeflemektedir. Fakat diğer bir gereksinim olan Hamiltonian çemberi labirent algoritmaları için hedeflenen bir çıktı değildir. Labirent tabanlı kalkan üretiminin önemli aşamalarından biri Hamiltonian

çemberi özelliğini sağlamayan kompleks labirent algoritmaları çıktılarını Hamiltonian çemberi koşulunu sağlar hale getirmektir. Bu koşulu sağlamak için N sayıda sütün ve kolona sahip olan algoritma çıktısı 2N sütün ve kolon sayısına çıkartılır. Sonrasında her bir yeni düğüm arasındaki bağlantı labirent algoritması çıktısı baz alınarak bağlanır. Bu bağlantı sonucunda Hamiltonian çemberi özelliğini sağlayan kompleks bir kalkan üretilmiş olur. Bu sayede üretilen tek katmanlı kalkan donanım saldırılarına karşın kullanılabilir hale gelmiştir. Bu tez kapsamında labirent üretimi için iki farklı algoritma kullanılmıştır. Bunlardan ilki "Minimum Spanning Tree (MST)" algoritmasıdır. MST problemi en temel graf teori konseptlerinden biridir ve bu yöntemle labirent üretimi kullanılan bir yapıdır. Bu yapıya ek olarak "Artifical Fish Swarm Algoritması (AFSA)" labirent üretimi için kullanılmıştır. AFSA oldukça etkili bir sürü zeka algoritmasıdır. Bu algoritma kompleks yapıda labirent üretimi için kullanılmaktır. Anlatılan labirent algoritmaları çıktılarından kalkan üretme algoritması sayesinde bu çıktılar ile üretilen kalkan yapıları Hamiltonian çemberi kriterini sağlamaktadır. Diğer bir kriter olan kompleks bir kalkan yapısının oluşturulması analizi için bir metriğe ihtiyaç duyulmuştur ve bunun için oluşturulan kalkan yapılarındaki yönlerin entropisi karmaşıklık metriği olarak kullanılmıştır. Bu metriğe göre oluşturulabilecek maksimum entropi değeri 1.00 bit olarak belirlenmiştir. Daha temel bir algoritma olan MST ile oluşturulan kalkanların entropi değeri 0.9'da kalırken AFSA ile üretilen kalkan yapılarının entropi değerlerinin 0.99 olduğu görülmüştür. Bu sonuca bakılarak karmaşık bir labirent üretmeyi sağlayan algoritmaların kullanılmasıyla kompleks bir kalkan yapısı oluşturulabilmektedir.

Bu tez kapsamında ele alınan diğer bir konu da çok katmanlı kalkan üretimidir. Gelişen donanım saldırıları yöntemleri sayesinde tek katmanlı kalkan yapıları Entegre Devre güvenliği açısından daha az güvenilir hale gelmiştir. Çok katmanlı kalkan yapısı bu donanım saldırılarına karşı daha etkin bir koruma sunmaktadır. Bu yapının oluşturulması iki tane tek katmanlı kalkan yapısının birbirine bağlanmasını baz almaktadır. Bu bağlantı sırasında tek katmanlı kalkan yapısı oluşturulurken göz önüne alınan karmaşıklık ve Hamiltonian çemberi gereksinimleri sürdürülmüştür. Çok katmanlı kalkan yapısını oluşturabilmek için öncelikle iki tane kompleks tek katmanlı kalkan yapısı oluşturulur. Bu kalkanların ortak bağlantı yolları belirlenir ve bu bağlantı yollarından birbirine bağlanır. Bu bağlantılar sayesinde kompleks ve Hamiltonian çemberi gereksinime uygun labirent tabanlı çok katmanlı kalkan yapısı oluşturulur. Bu yapı oluşturulurken belirlenen bazı koşullar dikkate alınmazsa istenmeye döngü yapıları oluşur. Bu istenmeyen döngü yapıları Hamiltonian çemberi koşulunun bozulmasına sebep olmaktadır ve engellenmemesi durumunda bit dizisi kontrol devresi işlevini yitirmektedir. Bu koşulları ortadan kaldırmak için döngü kontrol algoritması geliştirilip çok katmanlı kalkan üretimi aşamasına eklenmiştir.

Çok katmanlı kalkan yapısı elde edildikten sonra parçalı kalkan üretme algoritması da tez kapsamında tasarlanmıştır. Bu algoritma daha büyük alanları korumaya yönelik kalkan üretimini amaçlayan bir tasarımdır. Kalkan ile korunması planlanan büyük alan N yatay M düşey alana bölünür. Bu alanlar labirent tabanlı çok katmanlı kalkan yapısı oluşturma algoritmasının NxM defa çalıştırılmasıyla korumaya alınır. Bu yapı için NxM sayıda aktif kalkan yapısında kullanılan alt modüle ihtiyaç duyulmaktadır. Bu sayede korunması istenen alan NxM sayıda kalkan yapısıyla korunmuş olup donanım saldırılarına karşı daha dayanıklı bir yapı üretimi sağlanacaktır.

Tasarlanmış algoritmalar ile labirent algoritmalarının çıktıları kullanılarak Entegre Devrelere yapılan donanımsal saldırılara etkin bir çözüm yolu sunan labirent tabanlı çok katmanlı kalkan yapısı üretilmiştir. Bu kalkan yapısıyla birçok alanda etkin şekilde kullanılan Entegre Devre yapılarının içerisinde bulunan hassas veriler üçüncü kişilerden korunmuş olacaktır. Bu önlem de Entegre Devrelerin birçok alanda daha güvenilir bir şekilde kullanılmasına olanak sağlayacaktır.

İleri çalışma olarak ise, bu tez kapsamında tasarlanan büyük bir alanı birden fazla kalkan yapısıyla kaplama algoritması alt labirent yapılarının birbirilerine geçişli bir yapıda oluşturulmasına olanak sağlayan bir algoritma yapısına döndürülmesi halinde daha etkin bir koruma sağlanabilir.

# 1. INTRODUCTION

The IC sector has recently experienced tremendous growth and innovation. This has solidified the pivotal role of these microelectronic components across many technological domains. As the complexity and sophistication of ICs continue to increase, so does the volume and critical nature of the data they carry. This surge in significance has given rise to a concomitant demand for heightened security measures, especially in light of the realization that these ICs are entrusted with sensitive and confidential information.

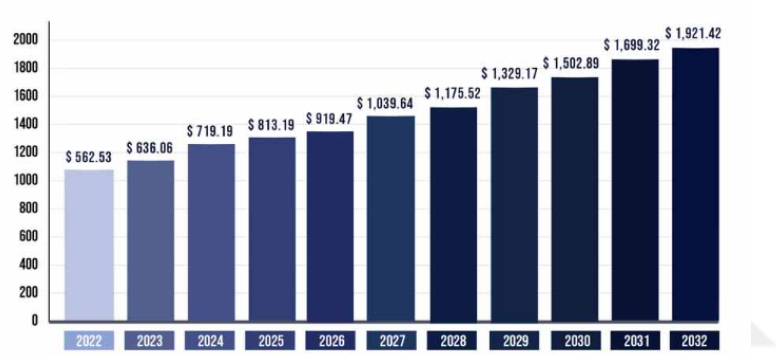



**Figure 1.1 :** IC Market Size, 2022 to 2032(USD BILLION) [1]

ICs are crucial to the functioning of various applications, from telecommunications to healthcare, finance, and national security. They hold valuable data, including personal user information and proprietary business intelligence. Therefore, it is essential to protect these ICs. As ICs become more integrated into our daily lives, addressing vulnerabilities that could compromise the integrity and confidentiality of the stored data becomes increasingly urgent.

One of the growing concerns in the field of technology is the vulnerability of ICs to hardware-based attacks. These attacks can exploit unnoticed weaknesses at higher levels of abstraction and can be classified into two categories: invasive and non-invasive. Non-invasive hardware attacks typically involve methods that do not require physical access and include analyzing side-channel information or software-based interventions. On the other hand, invasive hardware attacks usually involve physical access and interventions that target the internal structure of the IC.

In such attacks, the perpetrator often gains access to the circuit's internal components by opening the IC's outer casing or using microscopic needles. Chip Decapsulation, Microprobing, and Focused Ion Beam(FIB) Attacks are subcategories of invasive hardware attacks.

For the security of ICs, a physical shield structure can be employed against invasive attacks. This structure prevents attackers from obtaining confidential information within the IC. Through this shield structure, the continued effective use of ICs in technology can be ensured.

## 1.1 Literature Review

Utilizing the proposed physical shield structure against invasive hardware attacks is an effective defense method. The concept of a maze-based multi-layer shield is recommended for this protective structure. Based on a labyrinth design, the multi-layer shield aims to safeguard confidential data within ICs from invasive hardware attacks. The maze-based multi-layer shield structure aims to provide active shield protection on the Integrated Circuit. Active shield protection relies on a protection method that involves monitoring the uninterrupted flow of a bit sequence generated by a digital circuit through the employed shield. It ensures that the transmitted bit information from the input flows seamlessly through the entire shield, indicating no connectivity issues on the shield. The detection of any connectivity problem on the shield signifies a hardware attack. This approach ensures the protection of critical data within the Integrated Circuit.

Building a shield that works well must have three key features: complexity, connectivity, and full coverage. A maze-based structure provides the necessary complexity, while connectivity ensures data flows smoothly through the shield. Full coverage means that the shield must cover all the points in a graph. A shield is fully covered and connected when it satisfies the Hamiltonian cycle condition.

Shield designs meeting these criteria can be found in the literature [3] [4] [7]; however, the production of a maze-based shield represents a novel concept proposed within the scope of this thesis. The maze-based design aims to effectively defend against attacks on ICs by generating a complex pattern using the maze concept. This introduces a new

and innovative approach to designing shields specifically tailored to enhance resilience against attacks on ICs.

## 1.2 Hypothesis

This thesis proposes an effective method to protect ICs against invasive hardware attacks. It achieves this by utilizing maze algorithms to create complex shield structures that can be integrated into the Active Shield Architecture. The thesis advocates for the development of multi-layer shields instead of single-layer shields to enhance IC security. With these advancements, a multi-layer shield can be produced to provide effective protection against invasive hardware attacks. Moreover, the shield structure design can be integrated into the Digital ASIC Design Flow, making it a feasible structure for IC production.

# 2. BACKGROUND

## 2.1 Hardware Attacks

Due to their versatility and diverse applications, IC structures have become essential in many technological systems. With the rapid advancement of IC technology, these structures are now widely used in various fields, from computing and telecommunications to healthcare and security. Despite their benefits, the security of critical information stored within IC structures is a growing concern. As these structures are increasingly utilized in sensitive applications, the risk of unauthorized access and data breaches has become significant. Therefore, it is crucial to enhance the security measures of IC structures and ensure that critical information is adequately protected.

As technology advances, hardware attacks on ICs have become a growing concern for security experts. These attacks could lead to unauthorized access to sensitive data within a system, posing a significant risk to individuals and industries. This undesirable situation highlights the urgent need for enhanced security measures to prevent and mitigate the effects of such attacks.

Attackers often use hardware attack techniques to access critical data within IC structures. These techniques can generally be divided into two main categories: non-invasive and invasive hardware attacks. Non-invasive hardware attacks typically involve methods that do not require physical access, such as analyzing side-channel information or software-based interventions. On the other hand, invasive hardware attacks usually require physical access and involve interventions directed toward the internal structure of the IC. In such attacks, attackers often gain access to the internal components of the circuit by opening the external capsule of the IC or using microscopic needles, potentially allowing them to extract sensitive data. It is critical for organizations to be aware of these hardware attack techniques and implement measures to mitigate the risks associated with them.

### 2.1.1 Non-invasive attacks

Non-invasive hardware attacks refer to methods that do not require physical access to a device and involve analyzing side-channel information or software-based interventions. Side-channel attacks can be classified into different sub-types, such as Interference Attacks, Fault Injection Attacks, Electromagnetic Fault Injection, and Optical Fault Injection. These attacks aim to extract sensitive information from a device by analyzing side-channel information such as power consumption, electromagnetic radiation, or timing. Fault injection attacks aim to inject errors to disrupt the system's normal functioning deliberately. To prevent non-invasive attacks, measures should be implemented to make the analysis of side-channel information more challenging, protect side-channel information such as power consumption, electromagnetic radiation, or timing, and implement robust encryption methods.

### 2.1.2 Invasive attacks

An invasive hardware attack on ICs is a type of physical assault that involves gaining access to the internal structure of ICs and manipulating them. Attackers may use methods like altering components of ICs, reading or modifying memory contents, and cutting or manipulating connections, among others. The goal of such interventions may be to disrupt the functionality of ICs or gain access to sensitive information.

These attacks focus on the device's physical security and require advanced technical knowledge and hardware. By exploiting vulnerabilities in ICs, these attacks bypass other security measures put in place. Therefore, designing and producing ICs with security standards in mind plays a critical role in preventing such attacks.

### 2.1.3 Decapsulation

Decapsulation is a form of invasive hardware attack aimed at gaining access to the internal structure of a hardware device by physically removing its security measures. Attackers, by removing protective coatings or masks from the target device, directly access its internal components and may attempt to seize cryptographic keys by examining electronic components. This type of attack is typically conducted in a laboratory environment, and countermeasures are implemented through hardware security designs to mitigate its impact. Such attacks pose a potential threat to

the security of hardware used in critical applications, military systems, or essential infrastructures.

The first step in decapsulating a microchip is to remove it from the circuit board to make it easier to handle. Next, a cavity is carefully carved into the center of the IC package using a Dremel tool, as shown in Figure 2.1. This cavity should be deep enough to hold a drop of acid while ensuring the die below remains undamaged from the milling process.

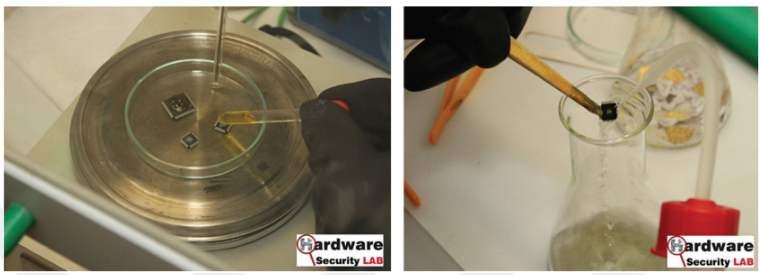



**Figure 2.1 :** Milling a cavity into the desoldered chip [2]

During the next step of the process, the chip is heated, and a drop of acid is applied to the milled cavity with great care. Usually, nitric acid or sulphuric acid is used for this process, as shown in Figure 2.2. After the reaction of the acid with the epoxy package has been completed, the chip is rinsed in acetone. Etch steps and rinse steps are repeated until the die is exposed. Depending on the type of attack, it is also possible to remove the package altogether by using this technique. In the case of invasive attacks, the chip needs to remain functional, and only the top epoxy cover of the chip is removed.

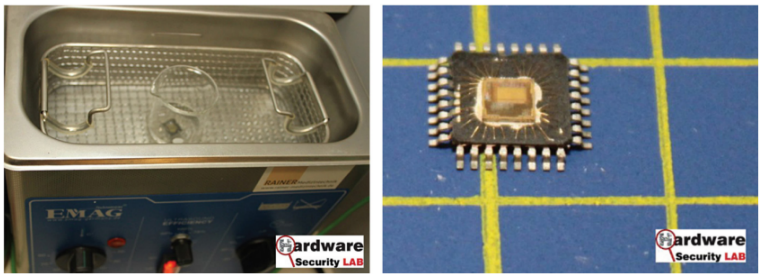



**Figure 2.2 :** Chip decapsulation with nitric acid (left), rinsing with acetone (right). [2]

### 2.1.4 Microprobing

Microprobing is an invasive hardware attack involving the use of micro-scale measurement tools to examine, measure, or modify the internal structure of ICs.

This kind of attack is usually carried out when ICs are physically accessible, and it involves making contact with the pins or connection points of ICs using specialized micro-probing devices, as in shown Figure 2.3 Microprobing analyzes signals within ICs, debug issues, or identify potential security vulnerabilities. Attackers can disrupt the functionality of ICs, gain access to internal information, or bypass security measures using this method. Therefore, to protect against such attacks, measures such as the physical security of ICs, secure design practices, and compliance with security standards should be taken.

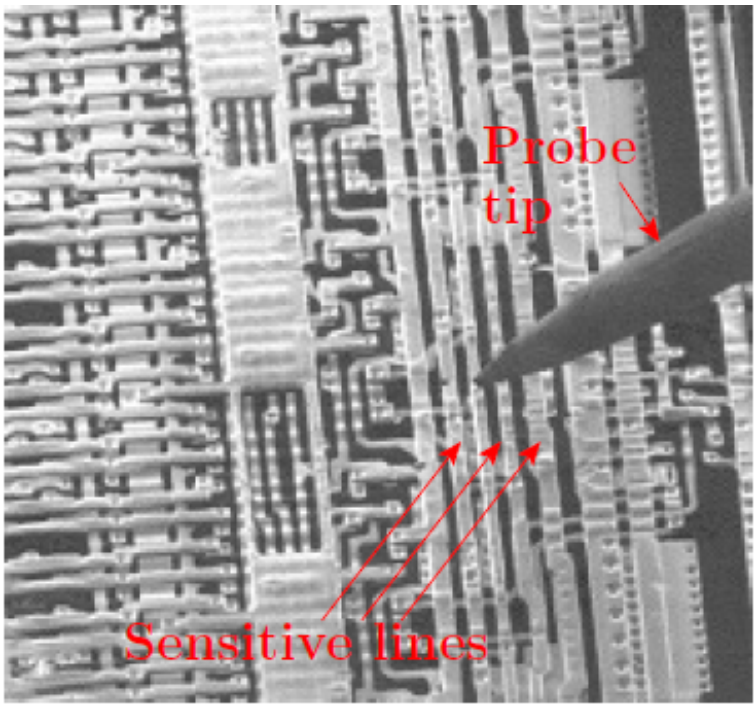



**Figure 2.3 :** Probing Attacks [3]

### 2.1.5 Focused ion beam (FIB)

FIB is an invasive hardware attack to compromise ICs. This involves using a focused ion beam to create small holes on the surface of ICs, as shown in Figure 2.4. FIB technology focuses an ion beam onto the material's surface, causing it to be sputtered or ablated.

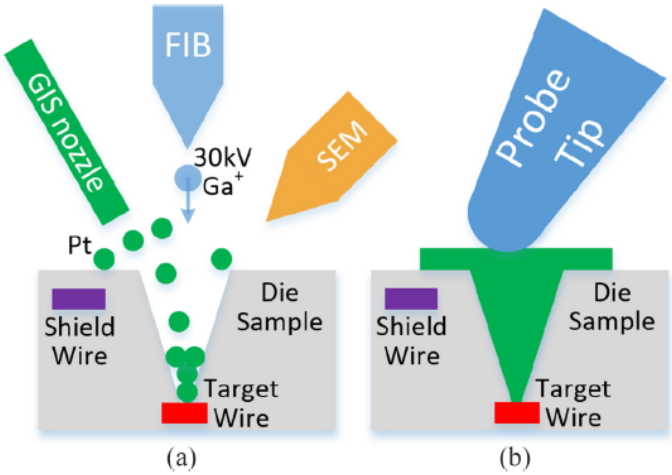



**Figure 2.4 :** (a) FIB deposits platinum in the milling cavity to build conducting the path from the target wire. (b) The deposited conducting path serves as an electrical probe contact. [4]

FIB attacks can be used to examine the internal structure of ICs, sever connections, manipulate components, or bypass security measures. The ion beam thins the surface material during the attack, allowing for detailed microscopic procedures. FIB attacks require specialized knowledge and expertise to overcome the physical security of ICs. Therefore, defenses against FIB attacks include physically protecting ICs and implementing security measures to make such attacks more challenging.

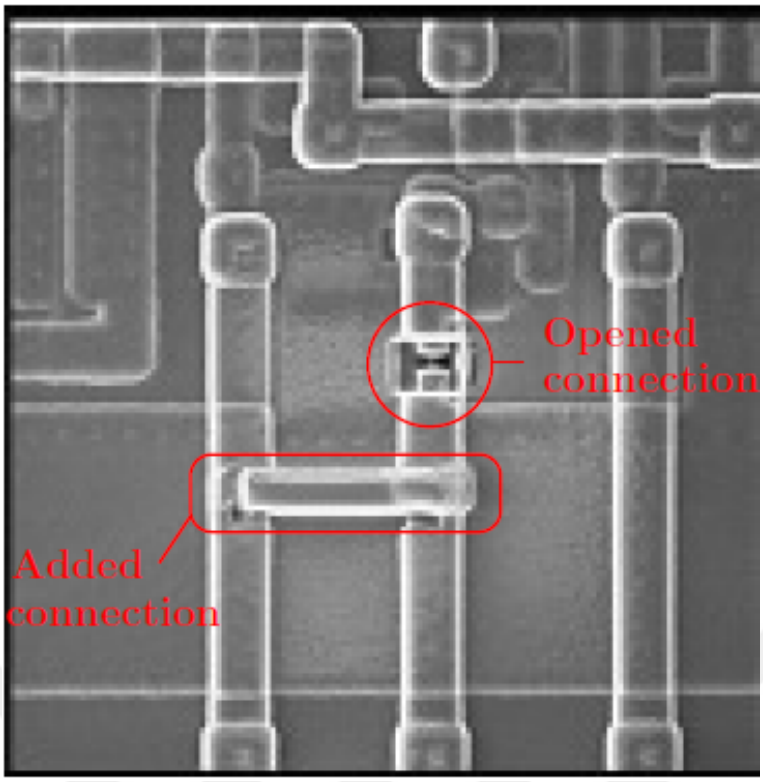



**Figure 2.5 :** Unlock the access to an internal memory thanks to FIB [3]

## 2.2 Active Shield Protection for Hardware Attacks

With the increasing sophistication of hardware attack techniques, safeguarding confidential information stored in ICs has become a significant concern. To tackle this problem, the shielding method offers an effective solution against hardware attacks that aim to extract data from ICs. The shielding solution covers regions not intended to be accessed by attackers with a shield structure. This physically prevents unauthorized access to sensitive data by attackers.

There are two techniques for shielding: Passive Shielding and Active Shielding. Passive shielding relies on analog shield integrity measurement and employs characteristics such as the capacitive load of a line to establish a unique signature. However, this approach has vulnerabilities as it must accommodate certain variations in the monitored quantity. On the other hand, active shielding is a more robust alternative. This methodology involves injecting random sequences of bits into the topmost metal circuit and subsequently verifying that these sequences remain unaltered throughout their journey.

### 2.2.1 Active shield architecture

Active shields are a crucial defense mechanism against invasive hardware attacks, aiming to make probing attacks more difficult, if not impossible [8]. Active Shield architecture provides high-level security against probing attacks. It consists of a bit checker, bit pattern generator, and shield structure, as shown in Figure 2.6, providing adequate protection against hardware attacks.

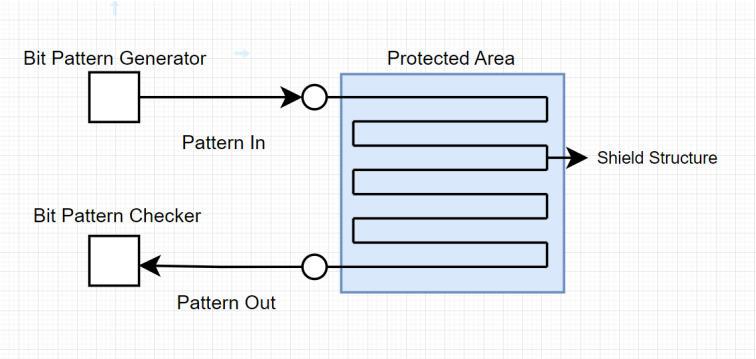



**Figure 2.6 :** Active Shield Architecture

The bit pattern generator module used in the Active Shield design is a subsystem controlled by digital circuits on the IC, responsible for creating a specialized protection pattern. This module generates a specific bit pattern using a proprietary algorithm or logical operations. The goal is to safeguard the internal structure of the IC and thwart unauthorized interventions. The bit pattern generator module forms a pattern by traversing specific components and regions of the IC. This pattern is designed to impede attackers from accessing sensitive data or causing damage to the IC. Typically designed in compliance with security standards, the module can enhance the IC's defense capabilities by incorporating various security layers. This bit pattern generator module can periodically update the designed pattern or dynamically alter it. This feature can increase security measures by making it more challenging for attackers to decipher or deceive the pattern.

The bit pattern checker module, employed in the Active Shield design, is a subsystem that monitors protection patterns generated by digital circuits on the IC. This module evaluates the state of the IC based on a defined protection pattern or bit pattern set and identifies undesired situations. The bit pattern checker module performs real-time comparisons with the designed security patterns by continuously monitoring specific

components and regions on the IC. If any alterations or errors in these patterns are detected, the module identifies the situation and can take necessary precautions. This module is designed to provide a more responsive and effective response mechanism against attacks. The bit pattern checker module includes customized algorithms and logical operations to assess the security status of the IC and continuously monitor protection patterns. The design aims to enhance the IC's security by offering an effective defense against potential threats.

The Shield structure is an essential sub-module in the Active Shield design responsible for protecting the most sensitive areas of the IC. The Bit Pattern Generator module generates a bit pattern that passes through this Shield structure before reaching the Bit Pattern Checker module. However, any potential attack during this process could compromise the system's security. To ensure the Shield structure can resist such attacks, it must meet specific requirements, including complexity, connectivity, and full coverage. These requirements are critical to the structure's ability to provide complete protection to the system.

### 2.2.2 Shield structure requirements

The shield structure is a crucial component of the Active Shield Architecture designed to protect against hardware attacks. This structure creates a physical barrier to safeguard ICs from such attacks. The quality of the shield structure is directly linked to the level of safety provided to ICs against hardware attacks. As the quality of the shield structure increases, so does the level of safety for ICs. To create a high-quality shield structure, three main requirements must be met: complexity, connectivity, and full coverage.

#### 2.2.2.1 Complexity

The complexity of a shield structure is a critical aspect to consider to protect sensitive information from attackers. Before attempting to access the information, attackers must first disable the shield. The structure should have a complex architecture to prevent it from being easily compromised. This complexity will make it difficult for attackers to obtain design information quickly.

Reverse engineering methods can be used to obtain detailed design information [4].This information makes it possible to identify the wires through which sensitive data passes within the IC. Advanced automatic tools, such as ChipJuice from Texplained [9] and pix2net from MicroNet [10] can automatically extract the netlist from each layer's images captured through optical or scanning electron microscopes (SEMs). This dramatically accelerates the reverse engineering process.

Through various analyses conducted, it has been determined that attackers can detect the shield structure. Attackers can easily bypass it by re-routing techniques if a simple shield structure is used, as shown in Figure 2.7. To execute this, the attacker will

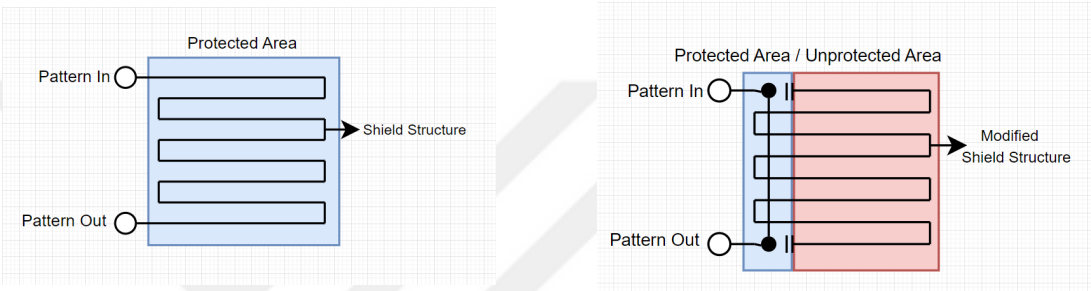



**Figure 2.7 :** Re-Routing Attack

leverage the FIB method to sever wires within the shield and add new connection paths. Once these modifications have been made, the pattern generated by the bit checker circuit flows through the modified shield to the bit checker module. Since there is no issue with the pattern, it cannot be detected that the IC is under attack. In such a scenario, the attacker can access sensitive data via microprobing. To safeguard against this attack method, the shield structure must have a complex architecture. This increases the difficulty level for attackers to analyze the shield and execute the re-routing attack.

#### 2.2.2.2 Connectivity and full coverage

To implement the Active Shield Architecture technique for a shield structure, it is crucial to establish connectivity between the input of the flowing pattern on the shield, the output of the bit pattern generator module, and the bit pattern checker circuit. This condition ensures that the pattern generated by the bit pattern generator module passes through the shield and reaches the bit checker module. This condition is

called Connectivity. Without satisfying this condition, applying the Active Shield Architecture to a shield structure is impossible. Therefore, it is necessary to carefully design and connect these components to achieve the desired result. To ensure that a shield structure fully protects an entire area, it is crucial that the structure passes through all nodes encompassing that area. If the shield structure does not cover all nodes, then complete protection cannot be achieved, and any areas that are left uncovered become potential target zones for adversaries. This is why the condition of having a shield structure that passes through all nodes is known as Full Coverage. It is necessary to ensure comprehensive protection against any potential threats or attacks. In the scope of this thesis, the Hamiltonian Cycle structure has been employed to meet these two shield requirements. A Hamiltonian Cycle is a concept in graph theory, specifically in the field of combinatorics. It refers to a cycle that visits every vertex exactly once in a graph. In other words, it is a closed loop that travels through each graph node without revisiting any node. If such a cycle exists in a graph, the graph is said to be Hamiltonian.

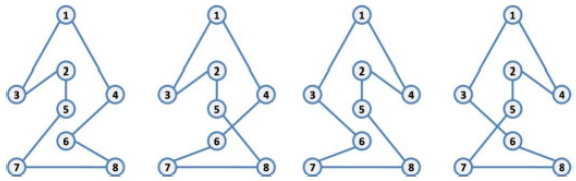


**Figure 2.8 :** Hamiltonian Cycles [5]

As a concept, the Hamiltonian Cycle is crucial in establishing a secure shield structure for ICs. The primary reason for this is that the Hamiltonian Cycle meets two of the most essential conditions for a reliable and effective shield: connectivity and full coverage.

The connectivity condition requires that the shield provides a continuous path for signals to travel from input to output. The closed-loop structure of the Hamiltonian Cycle satisfies this requirement, enabling a shield developed according to it to transmit signals seamlessly throughout the IC.

Another important requirement for a shield is full coverage. This means that the shield must cover all the nodes within the area it is meant to protect. The Hamiltonian

Cycle satisfies this requirement as it ensures that each node is visited only once, thus guaranteeing full coverage of the area.

Thus, a shield structure designed using the Hamiltonian Cycle effectively provides a shield and ensures that the shield covers all nodes within the IC. This makes the Hamiltonian Cycle an essential concept for IC designers to understand and implement to ensure the security and reliability of their designs.

The following sections of the thesis will discuss the conditions necessary to generate a shield. This will involve referencing the Hamiltonian Cycle condition for connectivity and full coverage.

## 2.3 Multi-Layer Shield Technique

One of the effective ways to protect the data is through the use of shielding, which can be applied in multiple layers to enhance the level of protection. By incorporating multi-layered shields, a more complex and comprehensive safeguard can be achieved compared to using a single layer. The transitions between the layers make it more challenging for attackers to analyze the shield structure and implement re-routing attacks by adding new connections from relevant locations. With this configuration, the fundamental aspects of shield analysis and attack become significantly more complicated. Overall, the multi-layered shielding method provides a more sophisticated and robust approach to safeguarding data within an IC.

FIB technology is a commonly used method for hardware attacks, which can potentially compromise the security of a system. However, the effectiveness of this technology is significantly reduced when dealing with a multi-layered shield structure. This is because the aspect ratio of FIB technology, which allows for the perforation of the IC and the addition of new connections or microprobing attacks on target wires, is greatly constrained by the multi-layered shield structure [4]. As a result, this multi-layered shield structure acts as an effective countermeasure against FIB attacks, making it difficult for potential attackers to breach the system's security. The precision of the drilling process in accessing a region with a single-layer shield structure differs from the precision of the drilling process in a multi-layered shield structure, as shown in Figure 2.9. This disparity contributes to an increased level of protection within the IC.

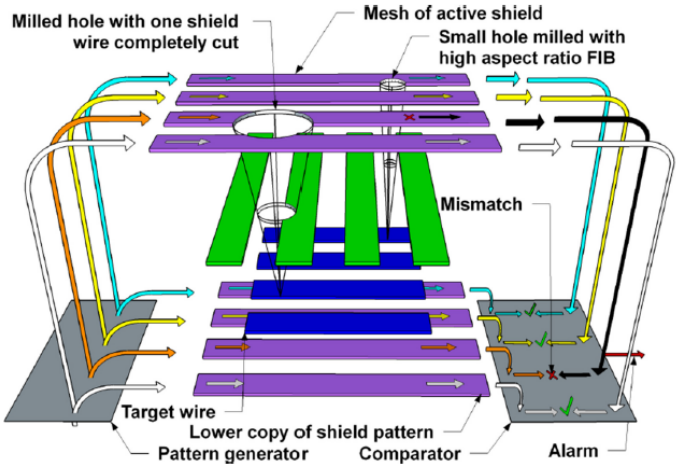



**Figure 2.9 :** FIB Attacks with different aspect ratio on Multi-Layer Shield [4]

# 3. GENERATION OF MAZE SHIELD TO ACTIVE PROTECTION AGAINST HARDWARE ATTACKS

## 3.1 Maze Based Shield

Maze algorithms are computational techniques used to create complex patterns known as mazes. These mazes are fascinating puzzles and can be used for practical purposes, such as improving the security of ICs against hardware attacks. In the context of IC security, maze algorithms are employed to generate shield structures. These structures act as a defense mechanism, fortifying the ICs against various hardware attacks. The resulting structures exhibit high complexity by incorporating maze-like patterns into the shield design.

This complexity makes it more difficult for potential attackers to analyze and manipulate the hardware, as they must contend with intricate patterns that obscure the underlying hardware architecture. The complexity of the generated shields is a crucial aspect of their effectiveness. The maze structures are advantageous in blocking hardware attacks because the complex nature of these mazes makes understanding and navigating them without proper knowledge or algorithmic guidance a formidable task. Maze algorithms ensure that the generated shields are complex and tailored to meet the specific requirements of IC protection. The algorithmic approach allows for the customization of shield structures, considering the targeted ICs' unique characteristics and potential threats they may face.

In addition to complexity, the Hamiltonian cycle condition is highlighted as an essential requirement for generating maze shields. The Hamiltonian cycle is a concept in graph theory that refers to a closed loop in a graph that visits each vertex exactly once. Enforcing the Hamiltonian cycle condition for maze algorithms for IC protection ensures a specific traversal pattern within the shield structure. By incorporating the Hamiltonian cycle condition, the maze shield is designed with a predetermined path that covers all essential components of the IC. This predetermined path ensures the shield provides comprehensive coverage, leaving no vulnerabilities unchecked. It

adds an element of systematic coverage to the complexity, making the shield not only intricate but also strategically structured for maximum protection.

### 3.1.1 Usage of maze algorithms for maze shield generation

The thesis presents a new concept called the "maze shield," which is a reliable method to protect sensitive data within ICs. Creating this protective measure relies on maze algorithms, which are crucial in generating a solid defense. The primary objective of these algorithms is to build a maze structure with significant complexity, as the quality of the resulting maze shield is directly related to the intricacy of the output.

Various maze algorithms are available to create maze structures, and the algorithm developed for generating a maze shield is designed to integrate different maze algorithms seamlessly. The maze generation process is seen as a sub-module within the maze shield flow. The output from maze generation algorithms undergoes slight modifications to align with the following steps of the maze shield algorithm. After these adjustments, the crucial phases of the maze shield algorithm are executed. This systematic flow allows the use of various maze algorithms, which increases flexibility in creating maze shield structures.

In addition, this adaptable design ensures the easy assimilation of developing maze algorithms. Newly created and quality-verified maze algorithm outputs can be integrated into the algorithmic flow with minor adjustments. This feature streamlines emerging algorithms' integration and facilitates the continuous improvement of maze shield structures.

To determine how effective maze algorithms are in creating maze shields, it's essential to have a relevant metric. The entropy of directions serves as a valuable and objective tool for systematically evaluating maze algorithms in crafting high-quality maze shields [3].This quantitative assessment enhances our understanding, guiding the refinement and optimization of maze-shield structures for superior performance in safeguarding ICs. The accurate calculation of this metric involves estimating the entropy of the directions, as indicated by equation (3.1), where P(d) represents the probability for the path in the direction of d. When the shield is only 2D, the Z direction P(z) probability equals zero. Then, 2D shield complexity is calculated by equation (3.2). The upper limit of the entropy is 1.000 bits for a 2-dimensional shield.

$$E(d) = \sum_{d\varepsilon\{x,y,z\}} -P(d).log_2 P(d) \tag{3.1}$$

$$E(d) = \sum_{d\varepsilon\{x,y\}} -P(d).log_2 P(d) \tag{3.2}$$

This thesis uses the Minimum Spanning Tree(MST), the fundamental concept in graph theory, and the Artificial Fish-Swarm algorithm (AFSA), considered one of the best swarm intelligence algorithms.

The Artificial Fish-Swarm Algorithm (AFSA) is a highly effective swarm intelligence algorithm first proposed in 2002 [11]. The diverse social behaviors and collective actions of fish inspired it. The algorithm works based on neighborhood search, where each individual artificial fish performs specific behaviors based on its current state and surrounding environment. This process is similar to the Hamiltonian cycle generation process, where each cycle searches its surroundings to identify cycles that can be merged. This makes the artificial fish-swarm algorithm very effective for optimizing the generation of the Hamiltonian cycle. The algorithm also maintains good randomness, which is essential for the random generation process of the Hamiltonian cycle. Therefore, the Artificial Fish-Swarm Algorithm is an ideal choice for optimizing the Hamiltonian cycle-generation process [7].

The Minimum Spanning Tree (MST) problem is a fundamental concept in graph theory and computer science. It involves finding a tree that connects all the vertices of a connected, undirected graph with the least possible total edge weight [12]. In maze generation, the MST problem creates a network of paths that links all maze areas while minimizing the total path length. By selecting edges with the lowest weights, a maze can be built where each passage is traversed with minimal cumulative distance. This approach guarantees a well-connected maze structure, with the MST algorithm serving as a valuable tool for creating mazes with optimized pathways and an overall balanced design.

This thesis uses two algorithms for maze generation: the Artificial Fish-Swarm Algorithm (AFSA) and the Minimum Spanning Tree (MST) algorithm. When the maze-shield algorithm is executed with the AFSA algorithm, the maze structure is visually depicted in Figure 3.1. This image shows the complex pathways and

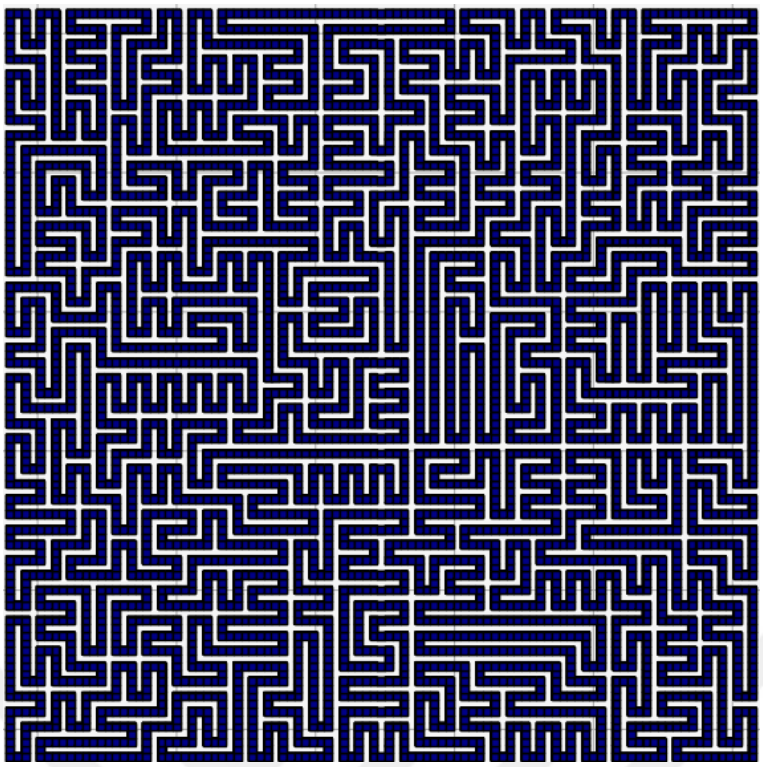


**Figure 3.1 :** Single Layer Maze-Shield with using AFSA

connections the AFSA algorithm forms, highlighting its effectiveness in generating maze structures with optimized configurations. On the other hand, running the maze-shield algorithm with the MST algorithm results in the maze structure shown in Figure 3.2. This image gives a visual insight into the maze generated by the MST algorithm, emphasizing its role in creating a well-connected network of passages with minimized total path length.

After analyzing the outputs of the maze-shield algorithm, it has been concluded that the Hamiltonian cycle requirement, which is crucial for creating a maze-shield, has been successfully met. However, it has been noticed that the maze-shield generated by the MST algorithm does not meet the complexity standards necessary for producing a top-quality maze-shield.

This is a matter of significant concern, as it implies that the structure of the maze-shield will be easily solvable through attacker analyses. If the maze-shield produced by the MST algorithm is utilized for IC security, it will result in a vulnerable structure for re-routing attacks. Consequently, attackers can quickly identify and exploit the points to be re-routed, giving them access to sensitive data that the user does not want third parties to obtain.

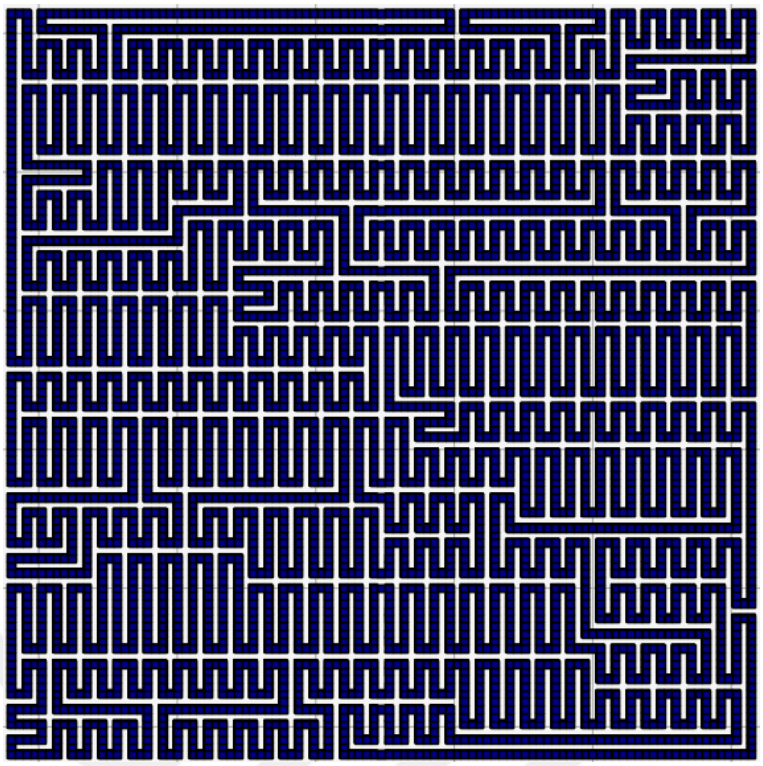


**Figure 3.2 :** Single Layer Maze-Shield with using MST

In contrast, it has been found that the AFSA algorithm, which is widely recognized as one of the best swarm intelligence algorithms, has generated a complex pattern that meets the complexity requirements necessary for creating a high-quality shield. Hence, when applied in IC protection, the maze-shield structure created with this algorithm will provide a maze-shield that is not easily analyzable by attackers, ensuring the protection of sensitive data.

Consequently, the utilization of maze algorithms that generate more complex mazes can significantly enhance the overall security of a maze-shield structure. This approach can be particularly beneficial in IC protection, where sensitive data is at risk of being accessed by unauthorized users. This approach can create a more complex and secure maze-shield structure that is far more resilient to potential security breaches. This is accomplished by introducing a maze-like path that must be navigated correctly to access the data, making it difficult for attackers to exploit the maze shield and gain unauthorized access to protected information. Thus, it is imperative to utilize maze algorithms that generate more complex mazes to create a more complex and secure maze-shield structure. This approach's enhanced security will make it more challenging for attackers to access sensitive data, ensuring its safety and integrity.

**Table 3.1 :** Entropy Results of Maze-Shield

| Used Algorithm | Size(RowxColumn) | Entropy(bits) |
|---|---|---|
| MSP | 50x50 | 0.8973 |
| MSP | 100x100 | 0.8974 |
| MSP | 150x150 | 0.9005 |
| AFSA | 50x50 | 0.9954 |
| AFSA | 100x100 | 0.9977 |
| AFSA | 150x150 | 0.9985 |

Table 3.1 provides the calculated entropy values based on the entropy equation (3.2). The MSP algorithm's maze-shield has a low entropy value because it does not have a complex structure. On the other hand, the AFSA algorithm's shields, known for enabling the production of complex maze-shield structures, have an entropy value that is very close to the maximum value of 1.00 bits.

### 3.1.2 Generation of maze shield

Although maze algorithms can generate visually complex patterns, they often fall short of meeting the requirements of the Hamiltonian cycle. The Picturesque technique [6] is a method that allows the creation of visually based mazes. This technique makes it possible to generate mazes in a desired shape. The method is inspired by the foreground creation technique, which is shown in Figure 3.3. An algorithm has been developed using this technique to construct a shield structure that complies with the Hamiltonian cycle condition. The algorithm uses the outputs of maze algorithms to create the structure. Figure 3.4 shows the generated of the shield structure by using the maze algorithm output. In Figure 3.4a, a group of points representing nodes is

**Algorithm 1** Maze-Shield Generation

**Input:** Number of nodes, Selected maze generation algorithm
**Output:** Single Layer Maze-Shield

```
Run selected maze generation algorithm
for All elements of maze generation algorithm outputs do
    Double all elements of maze algorithm outputs for Maze-Shield
end for
Create Maze-Shield using connections array generated with selected maze algorithm
```

displayed. These nodes are the starting points for maze algorithms that aim to generate complex maze patterns. The algorithms are designed to create complex connections between these nodes. The resulting maze structure from one such algorithm with nodes

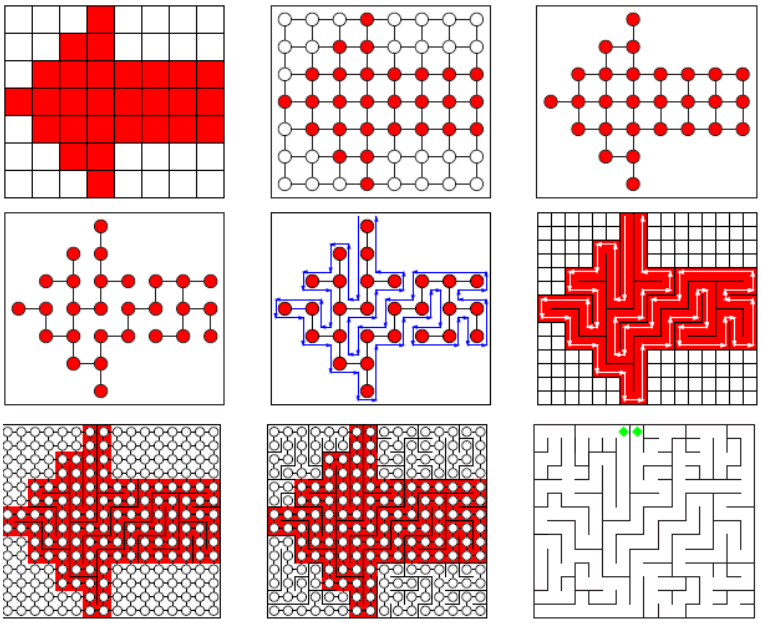
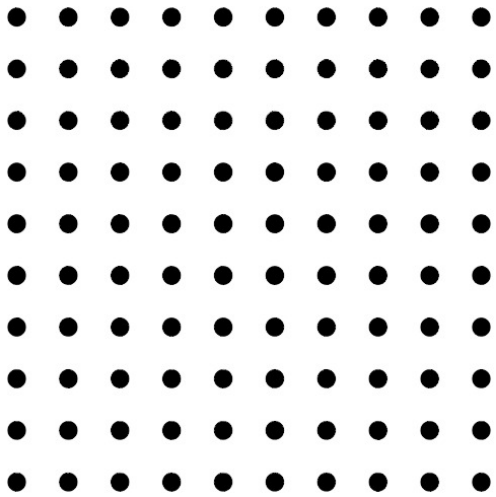
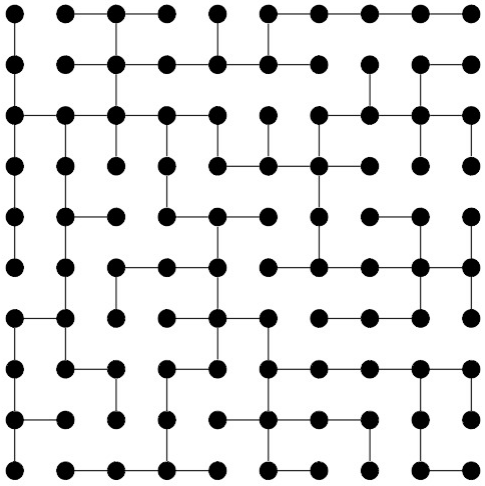


**Figure 3.3 :** The Foreground Generation Part of Picturesque Technique [6]

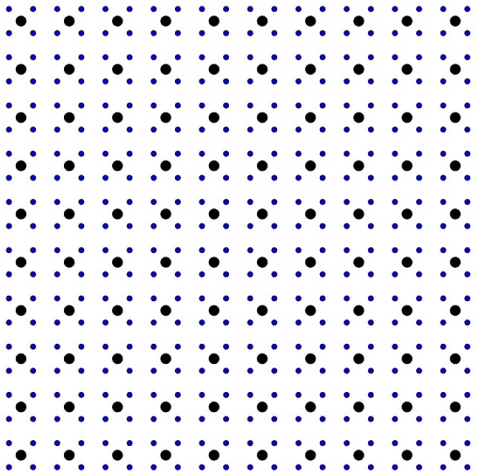
comprising ten rows and ten columns is demonstrated in Figure 3.4b. However, this maze structure needs to meet the Hamiltonian cycle condition. All nodes are initially replaced with four new connection points to satisfy this condition, as shown in Figure 3.4c. These new connections for each node are then established and connected. The necessary connection between neighboring points is established based on the node connections created by the maze algorithms. Some connections between points within the same node must be removed during this process. Once these steps are completed, the resulting outputs are shown in Figure 3.4d. The output of the maze algorithm applied to nodes consisting of ten rows and ten columns results in a maze-based shield structure with twenty rows and twenty columns.



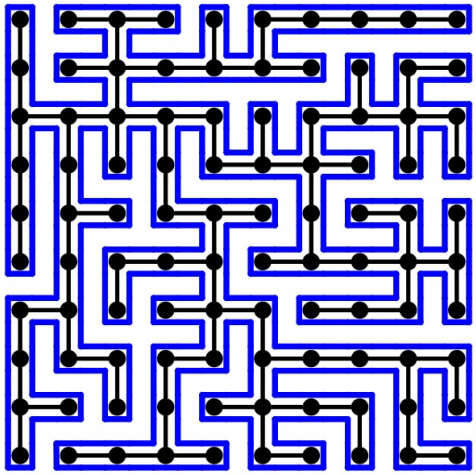
(a) Initial Nodes



(b) Outputs of Maze Algorithm



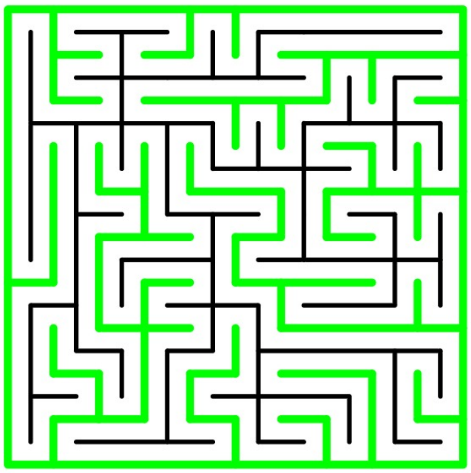
(c) Replacing Nodes to Generate Hamiltonian Cycle



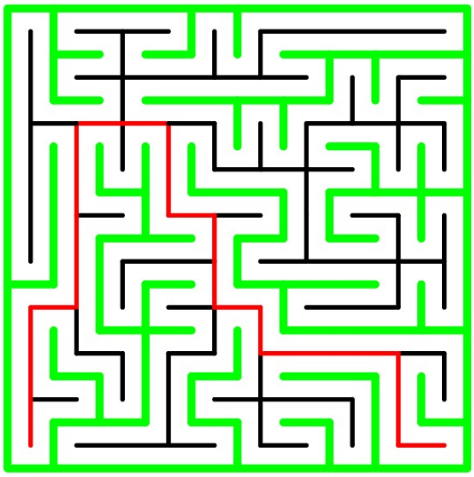
(d) Generated Shield

**Figure 3.4 :** Shield Generation with Using Maze Algorithm Output

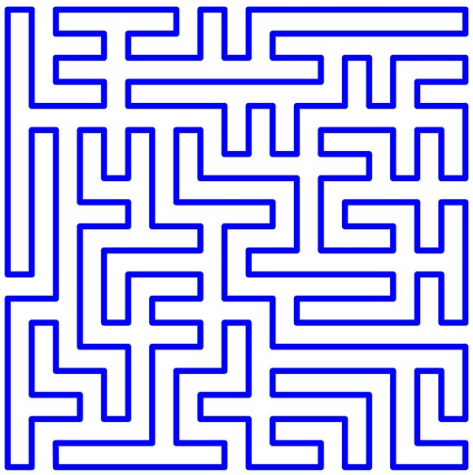
The process of generating a shield using the maze algorithm's outputs is illustrated in Figure 3.4. If the maze algorithm generates the same outputs, the resulting shield will look like Figure 3.5a. Furthermore, Figure 3.5b highlights one of the possible paths in the maze, and Figure 3.5c shows the shield generated using the outputs of the maze algorithm.



(a) Generated Maze



(b) Generated Maze and Maze Path Highlighted



(c) Generated Shield

**Figure 3.5 :** Generated Maze and Generated Shield

# 4. MULTI LAYER RANDOM MAZE SHIELD GENERATION AND VERIFICATION

## 4.1 Generation of Multi-Layer Shield

The technique of multi-layer shield connection is an effective method for fortifying IC against potential hardware attacks. This technique involves integrating multiple layers of shields, and its effectiveness depends on two key considerations: complexity and adherence to the Hamiltonian cycle condition. It is crucial to address the complexity aspect to ensure the efficacy of multi-layer shields. To achieve this, the technique utilizes a methodological approach. Two complex single-layer shields are employed as building blocks to generate a multi-layer shield. The complexity of each single-layer shield is designed to pose a formidable challenge to potential attackers. The resulting multi-layer shield inherits and amplifies the complexity of its constituent layers by combining two such complex shields. This layered complexity introduces a higher level of sophistication, creating a defense mechanism that is not only complex but also multi-faceted. The combination of complexities in the single-layer shields contributes to the overall resilience of the multi-layer shield against hardware attacks. The Hamiltonian cycle condition is an essential requirement for generating maze shields. This condition ensures a predetermined closed cycle within the shield structure that systematically covers all vital components of the IC. Maintaining the Hamiltonian cycle condition across layers becomes an essential process in multi-layer shields. The connectivity between the layers must be established to ensure the continuity of the predetermined path. This systematic path not only enhances the overall coverage of the shield but also actively contributes to the resistance against hardware attacks, as it ensures a comprehensive inspection of the entire hardware landscape.

A meticulous and dynamic process must be followed to establish a Hamiltonian cycle condition within a multi-layer shield. The process involves connecting two single-layer shields strategically through specific nodes that share connectivity in both shields. The connection is crucial for an uninterrupted path.

**Algorithm 2** Multi-Layer Shield Generation

**Input:** Two Maze-Shields
**Output:** Multi-layer Maze Shield

```
for All connections of Maze-Shield do
    Find all common connections between Maze-Shields
end for
Create random common connections list
for  All elements of random connections list do
    Complete VIA connection between Maze-Shields
    if Requirement of Maze-Shield connection(Loop Checker) == False then
        Remove VIA connection
    end if
end for
```

The first step in preparing a multi-layer shield is to identify nodes that share a common path connection in both single-layer shields. These nodes are chosen carefully for their role as critical connection points, ensuring the creation of a cohesive and unbroken traversal path.

Nodes with common path connections become potential connection points between the lower and upper shields. These nodes are the foundation of the IC, providing an uninterrupted path across its layers.

After identifying potential connection points, all possible connections are systematically and randomly listed. The intentional randomness in this order introduces an element of variability, guaranteeing the production of distinct multi-layer shields, even when utilizing identical pairs of two single-layer shields, as shown in Figure 4.1.

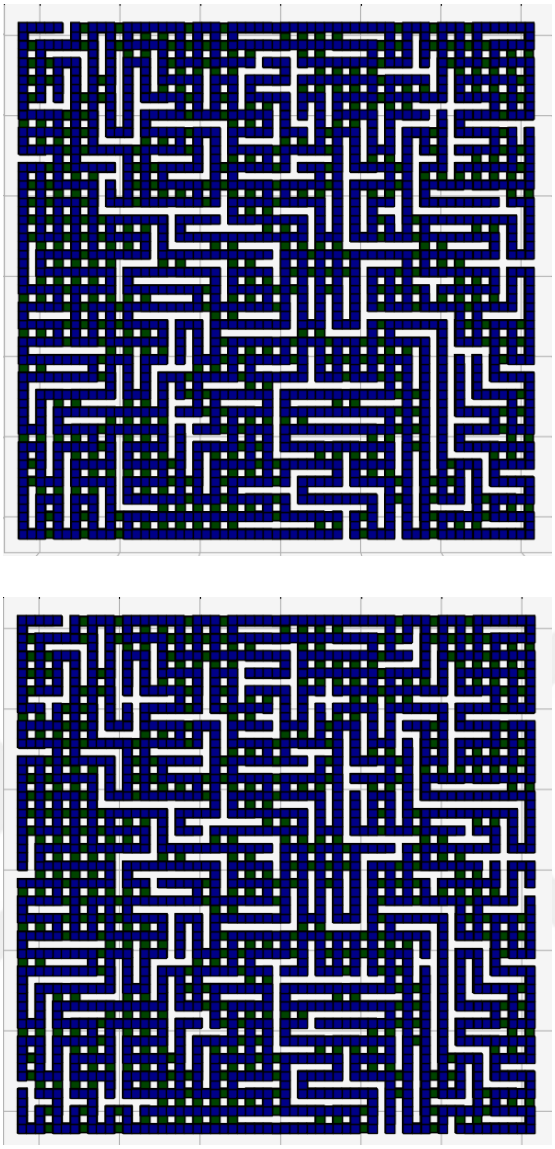
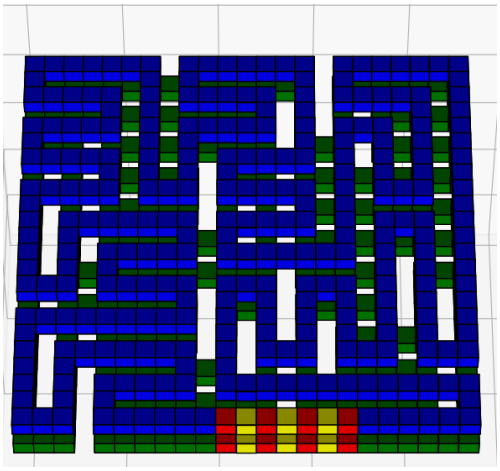


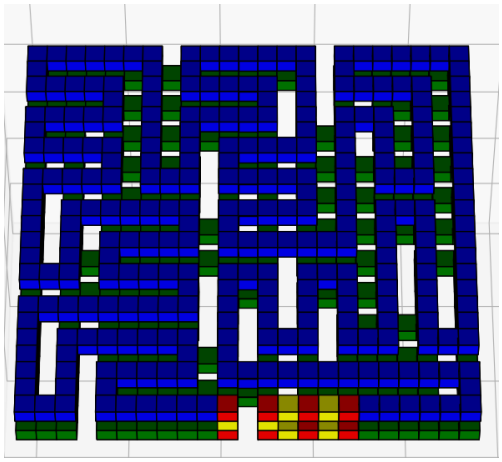
**Figure 4.1 :** Multi-Layer Shields Generated with Identical Single-Layer Shields

Connections between the lower and upper shields are initiated based on the randomly generated sequence. The unpredictability of this connection order ensures the generation of diverse multi-layer shields, showcasing the adaptability and versatility of the process. Following the random listing, connections are sequentially established based on the list of common paths. The method systematically removes these common paths and implements VIAs at the starting and ending nodes. VIAs serve as bridges, seamlessly interconnecting the lower and upper layers.

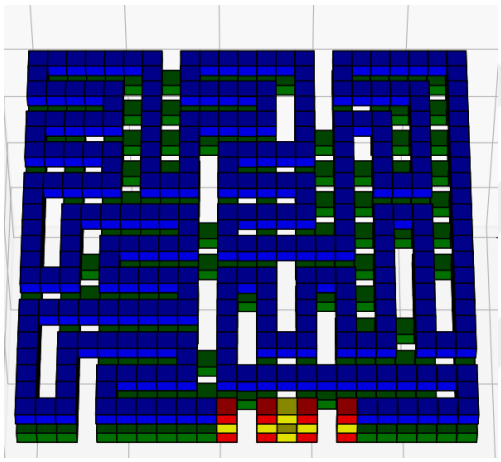
VIAs are strategically deployed at the starting and ending nodes of the common paths, ensuring a seamless transition and interconnection between the lower and upper layers. This approach enhances the continuity of the predetermined traversal path, establishing a robust and integrated defense.



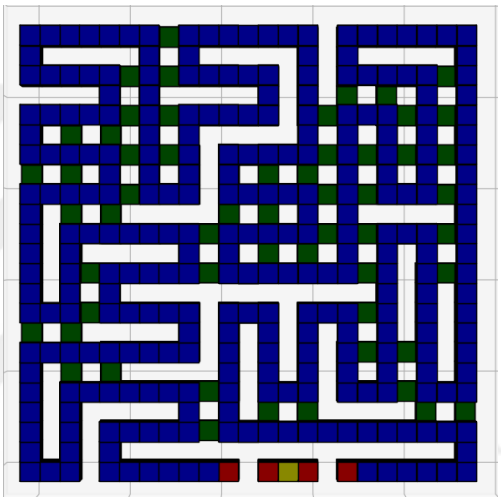
(a) Three Potential Connection Paths of Shields



(b) Shield after First Connection



(c) Shield after Second Connection



(d) Shield after Second Connection

**Figure 4.2 :** Forming Undesired Loop during Layers Connection Operation

Connections between upper and lower layers through nodes that share paths may not always lead to forming a multi-layer shield that satisfies Hamiltonian path conditions. ın some cases, a connection between the upper and lower layers can form an undesirable loop, as illustrated by the example discussed below. Figure 4.2a shows three possible connection points for such shields. The potential connection paths are highlighted in yellow, while the nodes are marked red for clarity. The layer connection algorithm has realized one of the possible connections, and the result is shown in Figure 4.2b. There are still two possible connections, and the layer connection algorithm can realize one of them to connect layers. After the connection operation, a connection between the upper and lower layers can form an undesirable loop, as shown in Figure 4.2c. This loop type is problematic because it disrupts the Hamiltonian cycle condition, which is crucial for the shield's effectiveness. It's important to note that if

one of the node pairs already has a VIA, the connection process may unintentionally create a loop. To prevent these unwanted scenarios, a loop checker algorithm has been implemented. The algorithm plays a vital role in maintaining the Hamiltonian path structure while connecting the upper and lower layers. The algorithm guarantees that the resulting multi-layer shield follows the Hamiltonian cycle condition by preventing the formation of loops. Moreover, the algorithm maximizes the number of connections while maintaining this condition, creating a more complex and resilient multi-layer shield structure.

## 4.2 Generation of Multi-Layer Shield Using Small Multi-Layer Shields

The multi-layer shield method is an effective approach to enhance security measures within an IC. This thesis proposes an algorithm for augmenting this method by incorporating small-scale multi-layer shields. The proposed algorithm divides the area to be safeguarded within the IC into N horizontal and M vertical sections. The multi-layer shield generation algorithm is then executed N times by M iterations, which results in the creation of NxM distinct multi-layer shields. Consequently, the targeted area is protected by NxM active shield architectures. This approach increases the complexity of the shield, making it more challenging for potential attackers to analyze and compromise the IC.

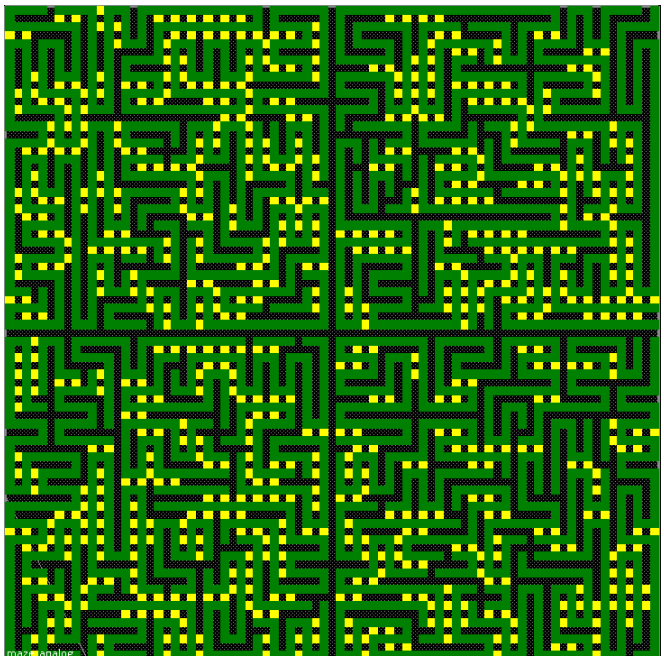


**Figure 4.3 :** The Shield Structure Generated with Four Small Shields

# 5. CONCLUSIONS

This thesis proposes using the maze-based multi-layer shield method against hardware attacks on ICs. To implement this method, first, the generation of a single-layer shield structure from the outputs of maze algorithms is explained. This explanation is realized using the AFSA and MST algorithms; their results are listed. Based on these results, a single-layer shield that can be used in the active shield architecture is produced using maze algorithms.

Following this stage, the production steps of the multi-layer shield structure, which is claimed to be more effective against evolving attack methods, are explained. As a result of this design, an effective defense system against advanced hardware attack methods is obtained. In addition to this system, an algorithm is designed to enable the production of a larger shield structure using the generated multi-layer shield structures. It is also explained that this design will be an effective solution against hardware attacks.

The designed maze-based multi-layer shield structure must be integrated into the Digital ASIC Design Flow to protect ICs against hardware attacks. The shield structure, which is integrated into the Digital ASIC Design Flow [13] for TSMC 65nm technology, is shown in Figure 5.1. The integration process indicates that it can be successfully realized when the enhanced shield structure is incorporated into the Digital ASIC Design Flow in a manner compatible with the desired technological framework.

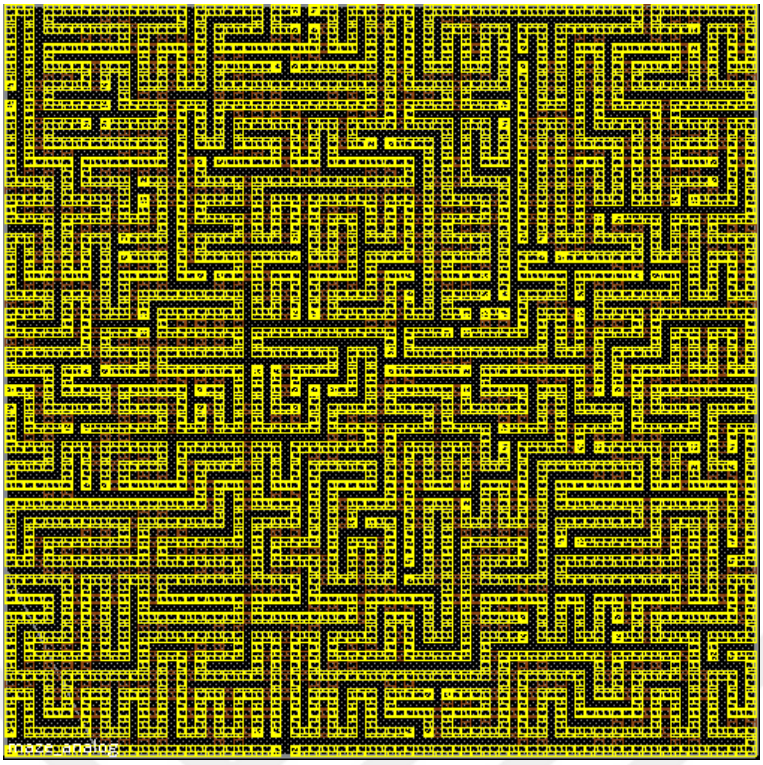


**Figure 5.1 :** The Shield Structure into Digital Design Flow

The proposed maze-based multi-layer shield structure is shown to create an effective protection system. As a future work, the algorithm that utilizes small shield structures to produce a large shield structure can be modified to an interleaved form. This way, an even more challenging shield structure can be obtained for attackers to analyze.

## REFERENCES


[1] https://www.precedenceresearch.com/integrated-circuit-market, date retrieved: 03.01.2024.

[2] **Hutle, M. and Kammerstetter, M.**, (2014). Resilience Against Physical Attacks, Smart Grid Security, Elsevier, pp.79–112.

[3] **Briais, S.**, **Cioranesco, J.**, **Danger, J.L.**, **Guilley, S.**, **Naccache, D. and Porteboeuf, T.** (2012). Random Active Shield, *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography*, pp.1–6.

[4] **Wang, H.**, **Shi, Q.**, **Nahiyan, A.**, **Forte, D. and Tehranipoor, M.M.** (2020). A Physical Design Flow Against Front-Side Probing Attacks by Internal Shielding, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, *39*(10), 2152–2165.

[5] **Wafdan, R.**, **Ihsan, M. and Suhaimi, D.** (2018). An Algorithm for Finding a Similar Subgraph of All Hamiltonian Cycles, *Journal of Physics: Conference Series*, *948*, 012063.

[6] **Yoshio Okamoto, R.U.** (2009). How to Make a Picturesque Maze, *Proceedings of the 21st Canadian Conference on Computational Geometry (CCCG2009)*, pp.137–140, http://cccg.ca/proceedings/2009/cccg09_36.pdf.

[7] **Xin, R.**, **Yuan, Y.**, **He, J.**, **Zhen, S. and Zhao, Y.** (2020). Random Active Shield Generation Based on Modified Artificial Fish-Swarm Algorithm, *Computers & Security*, *88*, 101552.

[8] **Cioranesco, J.**, **Danger, J.L.**, **Graba, T.**, **Guilley, S.**, **Mathieu, Y.**, **Naccache, D. and Ngo, X.** (2014). Cryptographically Secure Shields, *2014 IEEE Conference on High Assurance Systems Engineering*.

[9] https://www.texplained.com/about-us/chipjuice-software/, date retrieved: 03.01.2024.

[10] http://micronetsol.net/pix2net-software/, date retrieved: 03.01.2024.

[11] **Li, X.**, **Shao, Z. and Qian, J.** (2002). An Optimizing Method Based on Autonomous Animats: Fish-Swarm Algorithm, *Systems Engineering: Theory and Practice*, *22*(11), 32–38.

[12] **Mazeev, A.**, **, and Simonov, A.** (2017). A Distributed Parallel Algorithm for the Minimum Spanning Tree Problem, *Communications in Computer and Information Science*, pp.101–113.

[13] **Kurt, C. and Başkaya, F.** (2024). *Integration of a Maze Shield into Digital ASIC Design Flow for Hardware Attack Resistant ICs*.

**CURRICULUM VITAE**

**Raşit Rıdvan TURGUT:**

**EDUCATION:**

- **B.Sc.:** 2020, Istanbul Technical University, Electric Electronic, Electronic and Communication

**PROFESSIONAL EXPERIENCE AND REWARDS:**

- 2020-2022 TUBITAK Digital Design Engineer.
- 2022- Microelectronic Digital Design Engineer

**PUBLICATIONS, PRESENTATIONS AND PATENTS ON THE THESIS:**