

Low Cost and Effective Hardware Trojan Mitigation Techniques for Approximate Systems



By

Raja Muhammad Zohaib Tariq Kiani
(Registration No: 00000364133)

Department of Electrical Engineering

School of Electrical Engineering and Computer Science

National University of Sciences and Technology (NUST)

Islamabad, Pakistan

(Feb 2024)

Low Cost and Effective Hardware Trojan Mitigation Techniques for Approximate Systems



By

Raja Muhammad Zohaib Tariq Kiani

(Registration No: 00000364133)

A thesis submitted to the National University of Sciences and Technology, Islamabad,

in partial fulfillment of the requirements for the degree of

Masters of Science in

Electrical Engineering

Supervisor: Dr. Muhammad Imran

Co Supervisor: Dr. Rehan

School of Electrical Engineering and Computer Science

National University of Sciences and Technology (NUST)

Islamabad, Pakistan

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis entitled "Low-Cost and Effective Hardware Trojan Mitigation Techniques for Approximate Systems" written by Raja Muhammad Zohaib Tariq Kiani, (Registration No 364133), of SEecs has been vetted by the undersigned, found complete in all respects as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/M Phil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.

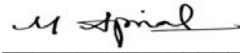
Signature: _____ 

Name of Advisor: Dr Muhammad Imran

Date: 13-Aug-2024

HoD/Associate Dean: _____ 

Date: 13-Aug-2024

Signature (Dean/Principal): 

Date: 13-Aug-2024

FORM TH-4

National University of Sciences & Technology

MASTER THESIS WORK

We hereby recommend that the dissertation prepared under our supervision by: (Student Name & Reg. #) Raja Muhammad Zohaib Tariq Kiani [364133]

Titled: Low-Cost and Effective Hardware Trojan Mitigation Techniques for Approximate Systems

be accepted in partial fulfillment of the requirements for the award of Master of Science (Electrical Engineering) degree.

Examination Committee Members

1. Name: Usman Khan Signature: 
04-Sep-2024 4:30 PM

2. Name: Muhammad Shahzad Younis Signature: 
04-Sep-2024 4:30 PM

3. Name: Rehan Ahmed Signature: 
04-Sep-2024 4:30 PM

Supervisor's name: Muhammad Imran Signature: 
04-Sep-2024 4:32 PM



Salman Abdul Ghafoor
HoD / Associate Dean

05-September-2024

Date

COUNTERSIGNED

05-September-2024
Date



Muhammad Ajmal Khan
Principal

Approval


It is certified that the contents and form of the thesis entitled "Low-Cost and Effective Hardware Trojan Mitigation Techniques for Approximate Systems" submitted by Raja Muhammad Zohaib Tariq Kiani have been found satisfactory for the requirement of the degree

Advisor : Dr Muhammad Imran

Signature:  _____

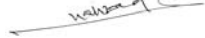
Date: 13-Aug-2024

Committee Member 1: Dr. Usman Khan

Signature:  _____


Date: 13-Aug-2024

Committee Member 2: Dr. Muhammad Shahzad
Younis

Signature:  _____

Date: 15-Aug-2024

Co-Advisor: Dr. Rehan Ahmed

Signature:  _____

Date: 13-Aug-2024

AUTHOR'S DECLARATION

I hereby declare that this submission titled "Low-Cost and Effective Hardware Trojan Mitigation Techniques for Approximate Systems" is my own work. To the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEecs or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEecs or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics, which has been acknowledged. I also verified the originality of contents through plagiarism software.

Student Name: Raja Muhammad Zohaib Tariq Kiani

Student Signature: uhqfBZ

Date: 13-Aug-2024

Certificate for Plagiarism

It is certified that PhD/M.Phil/MS Thesis Titled "Low-Cost and Effective Hardware Trojan Mitigation Techniques for Approximate Systems" by Raja Muhammad Zohaib Tariq Kiani has been examined by us. We undertake the follows:

- a. Thesis has significant new work/knowledge as compared already published or are under consideration to be published elsewhere. No sentence, equation, diagram, table, paragraph or section has been copied verbatim from previous work unless it is placed under quotation marks and duly referenced.
- b. The work presented is original and own work of the author (i.e. there is no plagiarism). No ideas, processes, results or words of others have been presented as Author own work.
- c. There is no fabrication of data or results which have been compiled/analyzed.
- d. There is no falsification by manipulating research materials, equipment or processes, or changing or omitting data or results such that the research is not accurately represented in the research record.
- e. The thesis has been checked using TURNITIN (copy of originality report attached) and found within limits as per HEC plagiarism Policy and instructions issued from time to time.

Name & Signature of Supervisor

Dr Muhammad Imran

Signature :



DEDICATION

This thesis is dedicated to family and friends.

ACKNOWLEDGEMENTS

Glory be to Allah (S.W.A), the Creator, the Sustainer of the Universe. Who only has the power to honour whom He please, and to abase whom He please. Verily no one can do anything without His will. From the day, I came to NUST till the day of my departure, He was the only one Who blessed me and opened ways for me, and showed me the path of success. There is nothing which can payback for His bounties throughout my research period to complete it successfully.

Contents

LIST OF TABLES	IV
LIST OF FIGURES	V
LIST OF SYMBOLS, ABBREVIATIONS AND ACRONYMS	VI
ABSTRACT	VII
1 Introduction and Motivation	1
1.1 Introduction	1
1.1.1 Problem Statement and Contribution	2
2 Literature Review	3
2.1 Approximate Computing	3
2.1.1 Security Challenges in Approximate Computing	4
2.1.2 Hardware Trojan in Approximate Circuits	5
2.2 Mitigation Technique for Trojan Detection in Exact Systems	6
2.3 Mitigation Technique for Trojan Detection in Approximate Circuits	7
3 Proposed Novel Techniques	9
3.1 A Partial Comparison Based Method against Hardware Trojans	9
3.1.1 Mitigating Hardware Trojan through Partial Comparison Method	10
3.1.2 The Partial Comparison Based Method	11
3.2 A Hybrid Based Method against Hardware Trojans	12
3.2.1 Mitigating Hardware Trojan through Hybrid Method	12
3.2.2 The Hybrid Based Method	13
4 Results and Discussion	15
4.1 Case Study	15
4.2 Hardware Performance Analysis	16

5 Conclusion	18
Bibliography	19

List of Tables

4.1 Area and Power of proposed Partial Comparison and Hybrid Techniques with Different Approximation Levels against Comparison based Method 17

List of Figures

2.1	Approximate Techniques at different levels [1]	4
2.2	Structure of Hardware Trojan	5
2.3	MV Technique to mask Trojan in Exact Systems[2].	7
3.1	Partial Comparison Method to mask Trojan in Approximate Systems .	9
3.2	Utilization of HT masking techniques against inputs A = 111111110 and B=11011010. Out1,Out2 and Out3 are outputs of three IPs from three different vendors(a) Comparison Technique [3] to determine intermediate value, (b) Partial Comparison Method to determine Intermediate Value, (c) Hybrid Technique to determine Intermediate Value .	10
3.3	Hybrid Technique to mask Trojan in Approximate Systems	12
4.1	Outcomes of an image enhancement for three approximate multipliers with different Hardware Trojans inserted, (a) the trigger condition of the hardware Trojan is 1×1 and the payload logic is to force the result to be 255, (b) the trigger condition of the hardware Trojan is 1×2 and the payload logic is to force the result to be 255, (c) the trigger condition of the hardware Trojan is 1×3 and the payload logic is to force the result to be 255, and (d) the image enhancement result of the approximate multiplier using the proposed partial comparison-based method (e) the image enhancement result of the approximate multiplier using the proposed Hybrid technique	16

LIST OF SYMBOLS, ABBREVIATIONS AND ACRONYMS

AC Approximate Computing
HC Hybrid Technique
HT Hardware Trojan
MV Majority Voting

Abstract

In the realm of computing, AC stands as a promising frontier, offering efficiency and speed. However, it has been reported in the technical literature that most of the existing AC designs are prone to hardware attacks. The recent research has unveiled the implications of neglecting security in approximate systems. The techniques to secure exact systems when fabricating chips with untrustworthy components are not applicable for approximate systems. The existing technique to mask the effect of Hardware Trojan (HT) in approximate circuits introduces significant area overhead and power consumption. Therefore, our paper presents novel design approaches to effectively mask the impact of HT, offering a significant 30% and 55% improvement in area and power efficiency, respectively. Our techniques strike a delicate balance, masking the Trojan threat while optimizing resource utilization. The effectiveness of proposed techniques is validated through a practical case study of image processing; three IPs with different HTs are successfully masked with a PSNR and SSIM of 33dB and 0.92 respectively. Through rigorous analysis and experimentation, we demonstrate the effectiveness of these techniques in strengthening security and improving reliability without compromising the efficiency of approximate computing systems. Our research seeks to throw light on the security challenges in approximate computing, while providing practical solutions to enhance security and reliability of these systems against potential threats while maintaining optimal performance.

Keywords: Approximate Computing, Hardware Trojan, Security Challenges, Reliability, Image Processing Application

Chapter 1

Introduction and Motivation

1.1 Introduction

In recent years, the AC has emerged as a promising paradigm to achieve computational accuracy by embracing imprecision within acceptable range. AC is a trade off between traditional accuracy and resource optimization which makes it a very promising tool for error tolerant applications. This approach harnesses the inherent imprecision within computations for better performance and power efficiency aligning with the demands of modern day computing applications.

AC engulfs a wide range of techniques and methodologies which include employing lower-precision data representations and utilizing various approximation strategies. The AC applications span a wide range of domains, including image and video processing, scientific simulations, and machine learning as discussed in [1]. This versatility positions AC as a valuable technology for scenarios where speed and resource optimization are paramount. In these domains, the focus shifts from achieving precise answers to optimizing computational performance and efficient power utilization.

The paradigm of Approximate Computing (AC) holds significant promise for increasing computational efficiency, yet its adoption introduces security vulnerabilities which originates from inherent imprecision in AC and the challenge of differentiating approximate outputs. This computational paradigm introduces security vulnerabilities as discussed in [4] which require careful considerations and proper mitigation. One notable security threat is the potential for information leakage, as adversaries may exploit the imprecise computations to glean sensitive data. Understanding and addressing these security challenges is of paramount importance to ensure implementation of approximate computing technologies.

The AC systems inherently introduce vulnerabilities, making them exposed to attacks particularly HTs. The HTs are malicious alterations to hardware components that can compromise system functionality and integrity. In the integrated circuit (IC)

design process, many companies rely on third-party Intellectual Properties (IPs) to expedite the development of their products. These third-party IPs involve unmanageable design and production processes, making them likely vectors for insertion of HTs by malicious vendors. Intriguingly, the security paradigm for AC differs significantly from that of exact computing. The AC system yields results with an inherent level of approximation, which makes traditional security mechanisms, such as Majority Voting (MV) for multiple IPs discussed in [3] less effective. The inherent imprecision in AC systems discussed in [5] complicates the detection of HTs because unpredictable and intrinsic errors during approximate execution may be indistinguishable from malicious modification of input data. Despite the fervent study of AC, the security aspects, especially in the realm of third-party IPs, have been notably neglected. The paper [3] introduces one such security measure the Comparison-Based approach which is based on the comparison of results from multiple IPs. The outputs of multiple IPs are evaluated and the intermediate result of three IPs is the output. The proposed techniques masks the HT and generates the correct output.

1.1.1 Problem Statement and Contribution

The comparison based approach, while it bolsters security, it comes at the price of increased area overhead and power consumption, offsetting the efficiency gains typically associated with AC. In order to address this challenge, this research paper introduces novel approaches to secure approximate systems—approximate arithmetic units as a case-study. A very limited technical literature is available on making approximate systems secure. Therefore, we put forward following technical contributions of the paper:

- The two novel designs i.e. Partial Comparison (PC) and Hybrid Technique (HC) have been proposed to mitigate the effect of HT while considering multiple IPs from different vendors.
- Experimental results indicate 30% improvement in area and 55% improvement in power efficiency compared to existing technique of comparison method introduced in [3]
- The proposed approaches are substantiated through a practical case study of image processing application, achieving a high PSNR of 33dB and SSIM of 0.92 while effectively masking HT.

In summary, this research contributes to the growing body of knowledge surrounding secure AC. It emphasizes the growing need for security and reliability in the context of AC applications, explores innovative solutions to address vulnerabilities, and furnishes practical evidence of their advantages. This research sets the stage for the wider adoption of secure and resource-optimized AC systems in an era where computational efficiency is paramount.

Chapter 2

Literature Review

2.1 Approximate Computing

AC stands as a promising paradigm in the realm of energy-efficient computing. The conventional computing approach emphasizing precision in calculations results in high energy consumption and significant area overhead. AC challenges this paradigm by introducing controlled imprecision, considering the fact that not all applications require exact computations. Approximate computing relies on the ability of many systems and applications to tolerate some loss of quality or optimality in the computed result[6]. This approach offers design benefits in terms of design area and power. This departure from strict precision allows for significant energy savings without compromising overall computational performance. As the overall energy consumption of computing systems continues to increase, the requirement of innovative solutions like AC become more important.

One notable domain where AC demonstrates its efficacy is in applications featuring intrinsic error resilience, such as multimedia processing. The paper [7] explains that in applications where accurate but not necessarily precise results are required, AC can be implemented at both the hardware and software levels. At the hardware level, less accurate yet more energy-efficient circuits or intentional reductions in supply voltage can be employed. Similarly, at the software level, certain non-critical computations can be strategically ignored, resulting in improved area and power efficiency. This approach to AC provides a dynamic framework for tailoring energy efficiency based on the specific requirements of diverse applications.

Figure 2.1[1] shows classification of approximate computing techniques. Within the software landscape, the concept of Approximate Software allows compilers to optimize program execution for energy efficiency. Approximate Architecture extends this adaptability to support approximate computing for traditional code running on general-purpose processors. These processors can be enhanced to selectively execute specific

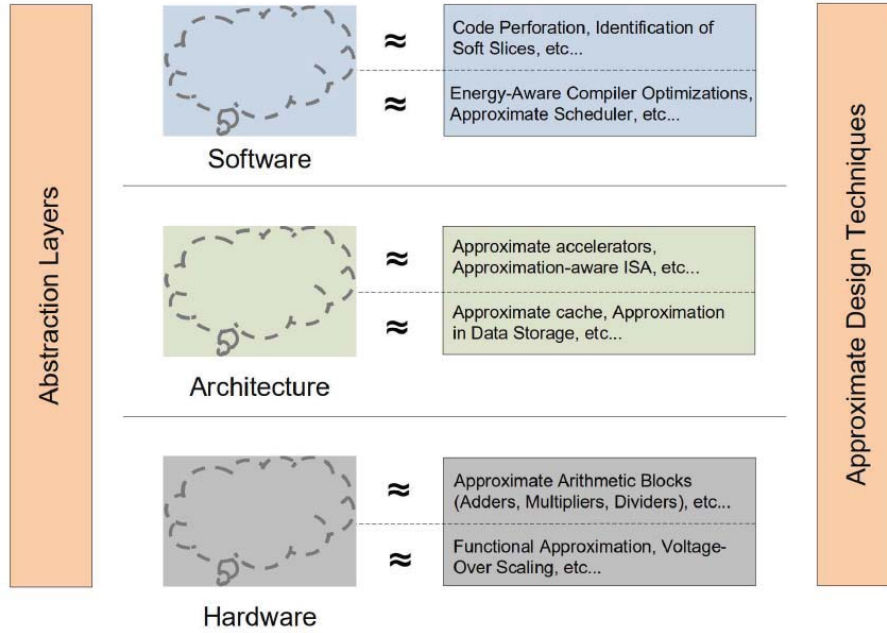


Figure 2.1: Approximate Techniques at different levels [1]

instructions or code segments in approximate mode, further contributing to energy efficiency. Additionally, the integration of Approximate Hardware transforms segments of traditional code into neurally inspired algorithms, executing them on specialized accelerators for improving energy efficiency[7]. This comprehensive approach positions AC as a fundamental player in reshaping the landscape of energy-efficient computing paradigms.

2.1.1 Security Challenges in Approximate Computing

While Approximate Computing (AC) holds great significance in achieving computational efficiency, its security and reliability implications are yet to be fully explored. The imprecise nature of approximate computations introduces inherent uncertainties, raising concerns about the reliability of results and the potential vulnerability to security threats. Utilizing AC systems in security-sensitive applications poses a significant challenge, necessitating a thorough understanding and mitigation of these issues before widespread adoption.

The uncertainties and unpredictable intrinsic errors during approximate execution may be indistinguishable from malicious modifications of input data, the execution process, and the results[8]. Any error that goes beyond the defined threshold or acceptable range in approximate systems will be considered as a potential malicious attack.

However, it is difficult to characterize errors as different approximate computing mechanisms most likely will generate errors with different characteristics.

Protecting the intellectual property (IP) embedded in Integrated Circuit (IC) designs has emerged as a concern for fabless semiconductor design houses[9]. As defenders intensify their efforts to safeguard critical circuit portions, attackers are concurrently developing increasingly sophisticated tools to extract valuable information and reverse engineer the functionality of these designs. The present day supply chain is distributed across multiple companies across different countries, thus exposing IPs to established security threats: overproduction, counterfeiting and malicious modifications. Careful consideration is required when using third party IPs in our design.

2.1.2 Hardware Trojan in Approximate Circuits

The HT is a form of malicious circuitry or addition to a design that damages the reliability or trustworthiness of a system. These Trojans are intended to disrupt the normal operation of a device. HTs can be inserted at various stages of the supply chain, including during manufacturing, design, or distribution[10]. A Hardware Trojan consists of trigger and payload as shown in Figure 2.2.

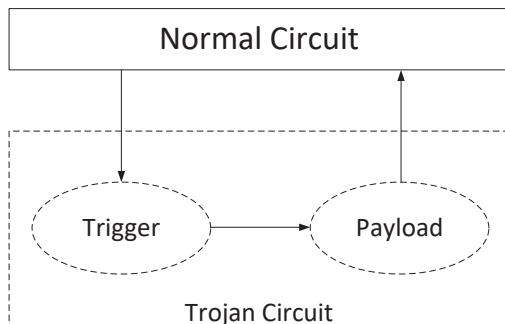


Figure 2.2: Structure of Hardware Trojan

Instances of HTs have been identified in fabricated chips within manufacturing industry chains, particularly in chips produced by untrusted foundries. These HTs, although manifesting with inconsiderable footprints, have the potential to disrupt the functionality of approximate circuits under rare circumstances. The intersection of approximate circuit designs and security vulnerabilities highlights the need for a more comprehensive examination of the potential risks associated with the adoption of AC methodologies.

Nowadays, third parties have been widely involved in IC designs and manufacturing in supply chains. From the design of IC chips to the process of manufacturing, these

outsourcing companies can purposely add malicious circuit logic units to circuits, also known as "hardware Trojan". HTs have been recognized as one of the most harmful attacks in hardware circuits. HTs can be added to the original circuit in the form of bypass circuits, and can be used to destroy circuits or steal data under the control of an attacker. Adversaries can maliciously change or add additional functionality of an IC using HTs. Since approximate circuits are available to an untrusted foundry in fabrication, hardware Trojans could be inserted, and then the inexact design of the approximate circuits may bring more opportunities for attackers[10] which makes it necessary to analyze and mitigate effects of HT in approximate circuit.

2.2 Mitigation Technique for Trojan Detection in Exact Systems

In the world of computing, hardware security and reliability is of great importance and we need to protect ICs from malicious tempering. The HTs covertly inserted into IC design pose a great threat to integrity and functionality of system. In technical literature, very limited techniques have been proposed to mitigate HTs in exact systems. One such technique proposed in [2] is Majority Voting

MV is a technique to mask the Trojan in exact systems. It is based on vendor diversity mechanism. Vendor diversity in the acquisition of Intellectual Properties (IPs) helps to mitigate potential security threats particularly those posed by HTs. When IPs are sourced from multiple vendors, the unique nature of HTs serves as a robust defense mechanism against coordinated attacks[11]. The utilization of IPs from different vendors help protect against the vulnerabilities associated with a single malicious vendor. MV helps restoring the correct circuit results even in the presence of potential discrepancies[12]. The redundancy introduced by diverse IP ensures continuous operation of logic elements which helps prevent availability attacks, such as Denial of Service (DoS). In essence, leveraging IPs from different vendors provides a robust defense against potential threats and attacks.

MV technique utilizes odd number of unreliable IPs and works by verifying output of each IP on bit by bit basis and performing a valid vote to generate the correct result. The output that is agreed upon by the majority is considered the valid result, mitigating the potential influence of faulty or malicious IPs. Figure 2.3 shows the majority voting mechanism when three different vendors are involved. Each Intellectual Property (IP) module contributes four outputs labelled as a0, a1, a2, and a3 where each output engages in a voting process by comparing its corresponding bits with those of the same position from other IPs. The final result is derived through a collective voting mechanism that synthesizes the individual contributions of each IP.

[11] and [12] takes the assumption that all IPs will have different trojan which is practical because the IPs came from different sources and its realistically difficult to

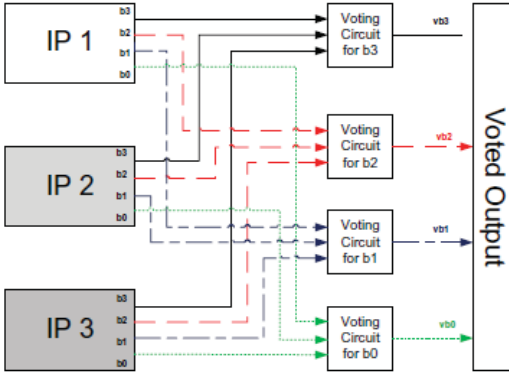


Figure 2.3: MV Technique to mask Trojan in Exact Systems[2].

design HTs from different sources.[11] and [12] employed vendor diversity and voting circuit to mitigate this threat. This is an efficient way to mitigate trojan but this requires purchasing different IPs having the same function from different vendors which is not possible for approximate circuits because approximate circuits from different vendors have different error characteristics as they don't have a uniform truth table because users of approximate circuits want their result to be within acceptable range rather than to be accurate.

2.3 Mitigation Technique for Trojan Detection in Approximate Circuits

To the best of author's knowledge, Comparison Method proposed in [3] is the only method proposed in technical literature to mitigate the effect of HT by giving intermediate result as an output of the three third party IPs. Comparison based technique was proposed in [3] to mask the trojan in approximate systems by giving intermediate result as an output of the three third party IPs.

The paper [3] discusses when a system is compromised by HT, the effected output may be the maxima or minima of the three outputs of three IPs. However, intermediate result of output of the three IPs always falls within the acceptable bound and yields the correct output masking the trojan. Comparison method involves bit by bit comparison of all IPs to generate intermediate result.

However while this method shows promise in mitigating HT, this brings along its own set of issues. One of the most significant drawbacks of comparison based technique is substantial area overhead and increased power consumption. These penalties undermine the prime purpose of AC which is effective resource utilization and optimal performance.

In our comprehensive literature review on approximate computing, we explored the versatility of this paradigm in various error-tolerant applications. MV technique while being efficient for trojan detection in exact systems has not proven to be effective for approximate systems. The unique characteristics of approximate computations demand alternative techniques, and, so far, the comparison-based approach stands out as the primary method for generating correct output when leveraging multiple IPs to mitigate HT in approximate systems. Nevertheless, the pursuit of efficiency in terms of area and power consumption in the presence of multiple IPs within Approximate Circuits (ACs) remains an active area of research. Further contributions are essential to improve existing techniques and developing novel approaches to mitigate trojan in approximate systems.

Chapter 3

Proposed Novel Techniques

This section introduces two novel methods Partial Comparison(PC) and Hybrid Technique(HC) against the insertion of Hardware Trojan in approximate circuits while keeping the output reliable and trustworthy.

3.1 A Partial Comparison Based Method against Hardware Trojans

The PC is based on strategic refinement of the conventional comparison based approach. Therefore, instead of performing comparison on every bit of multiple third party IPs, this technique selectively compares a subset of bits as shown in Figure 3.1.

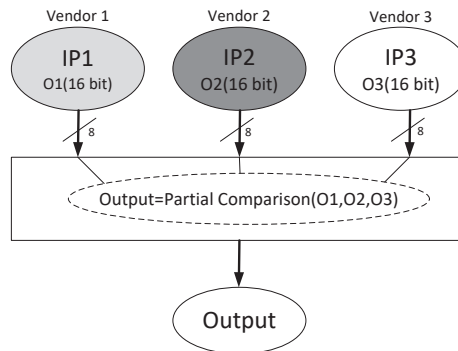


Figure 3.1: Partial Comparison Method to mask Trojan in Approximate Systems

3.1.1 Mitigating Hardware Trojan through Partial Comparison Method

As discussed earlier, the intermediate result of output of three IPs is always within acceptable range yielding the correct output and masking the HT as the effected output will either be maximum or minimum of output of three IPs.

In making our approximate systems reliable, we acknowledge the effectiveness of using intermediate results but recognize the challenge posed by existing methodology of area and power overhead due to extensive bit by bit comparison which makes the technique less viable for resource efficient applications. Our technique addresses this challenge by comparing only a subset of bits to determine intermediate value.

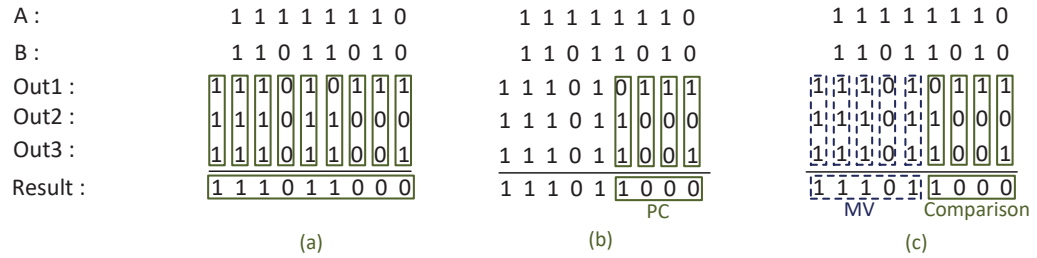


Figure 3.2: Utilization of HT masking techniques against inputs A = 111111110 and B=11011010. Out1, Out2 and Out3 are outputs of three IPs from three different vendors (a) Comparison Technique [3] to determine intermediate value, (b) Partial Comparison Method to determine Intermediate Value, (c) Hybrid Technique to determine Intermediate Value

Figure 3.2 illustrates our proposed PC technique against conventional comparison based method against inputs A=254(Dec) and B=219(Dec). Out1, Out2 and Out3 are outputs of three IPs from three different vendors. It can be seen that while conventional comparison based approach [3] involves bit by bit comparison to determine intermediate value(472), our approach efficiently determines intermediate value(472) by only comparing a subset of bits. In this way, balance between security and resource efficiency is achieved. This subset-based comparison methodology enables the generation of intermediate results while significantly reducing area and power consumption. The strategic partial comparison based approach not only masks trojan manipulation but also minimizes computational load making our technique a promising approach in the realm of secure and efficient AC systems

3.1.2 The Partial Comparison Based Method

The Algorithm 1 elaborates the working principal of PC. The A1, A2 and A3 are the inputs coming from three approximate IPs of three vendors and O is the output median result (Line 1/2 in Algorithm 1) d The algorithm takes the output of three IPs, i.e., A1, A2 and A3 as inputs (Line 1 in Algorithm 1). Initially, the LSBs comparison of the first two inputs (A1 and A2) is performed. and store the results to two variables, m1 and m2. (Lines 4-11 in Algorithm 1). The m1 contains the smaller value of the two inputs while m2 has the greater value among the two inputs. The m1 and m2 are then compared with the third input, i.e., A3 and then the intermediate value of the three inputs is decided to be the output by PC technique (Lines 12-21 in Algorithm 1).

Algorithm 1: Partial Comparison PseudoCode

```
1 Input : A1, A2, A3 — Coming from 3 IPs
2 Output : O — the result
3 Define variables m1 and m2
4 for  $i = 1$  : half bits of input do
5   if  $A1[i] \geq A2[i]$  then
6     |  $m1 = A2$ ;
7     |  $m2 = A1$ ; — m1 is smaller of the two inputs
8   else
9     |  $m1 = A1$ ;
10    |  $m2 = A2$ ; — m2 is larger of the two inputs
11  end
12  if  $m1[i] > A3[i]$  then
13    |  $O = m1$ ;
14  else
15    | if  $m2[i] > A3[i]$  then
16      |  $O = A3$ ;
17    | else
18      |  $O = m2$ ;
19    | end
20  end
21   $O$  is the Hardware Trojan free output
22 end
```

3.2 A Hybrid Based Method against Hardware Trojans

In the pursuit of securing Approximate Computing (AC) systems from the threat of Hardware Trojans, the HC emerges as a comprehensive and innovative approach by utilizing both MV Technique and Comparison based Technique to mitigate effect of Hardware Trojan. Comparison based technique is applied on lower bits while MV technique is applied on higher bits as shown in Figure 3.3

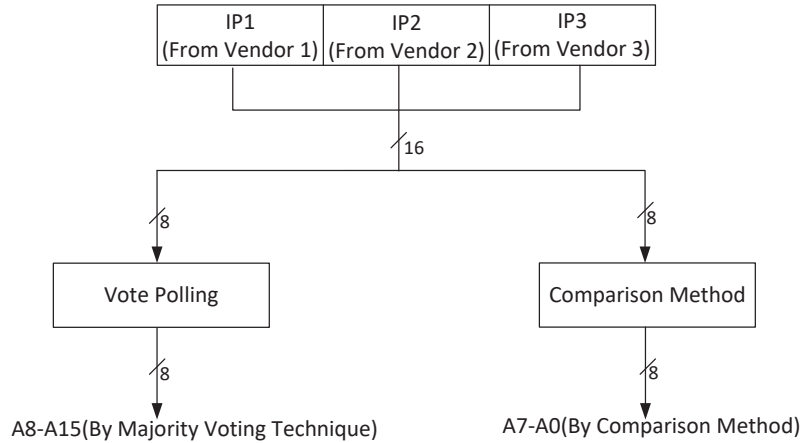


Figure 3.3: Hybrid Technique to mask Trojan in Approximate Systems

3.2.1 Mitigating Hardware Trojan through Hybrid Method

The paper [3] explains the challenges when MV technique is applied to approximate systems. The paper [3] discusses that applying MV technique in approximate systems yield unacceptable results because voting output offset surpasses the maximum output offset. Voting Output Offset is difference between the result obtained by voting mechanism and the exact result for a given input. Maximum output offset is maximum difference between the output of the arithmetic unit and exact result for a given input. Moreover as discussed in paper [3], approximate IPs from different vendors generate disparate result even with similar error metrics which makes MV inefficient against HT in approximate circuits.

In response to these limitations our proposed methodology, HC embraces an innovative approach to mask the approximate system from Hardware Trojan while maintaining computational efficiency. The inherent stability of MSBs is employed in our

proposed approach. MSBs from different vendors consistently align which maintains the integrity of computation. The HC applies MV on MSBs while applying comparison based method to the more susceptible LSBs. The HC ensures balance between the reliability of MSBs and precision offered by LSBs. Figure 3.2 illustrates our proposed HC technique against conventional comparison based method against inputs A=254(Dec) and B=219(Dec). It can be seen that HC employs MV on inherently stable MSBs and comparison on LSBs to determine intermediate value(472). The Hybrid based approach generates intermediate result while being resource efficient both in terms of area and power consumption. The reduction in number of compared bits translates to reduced area overhead and power consumption making Hybrid technique very effective in resource efficient applications.

3.2.2 The Hybrid Based Method

A1,A2,A3 are defined as the three outputs of approximate circuits from three vendors. The proposed Hybrid Method is shown in Algorithm 2. The algorithm takes the output of three IPs, i.e., A1, A2 and A3 as inputs (Line 1 in Algorithm 2). The algorithm computes bit level majority result from MSBs (Lines 4-13 in Algorithm 2). m1 constitutes MV result. The algorithm then performs comparison on LSBs to generate comparison result (Lines 14-31 in Algorithm 2). O1 constitutes LSBs from comparison method. Majority result (m1) and comparison result (O1) are concatenated in the end to generate intermediate result (Line 32 in Algorithm 2).

Algorithm 2: Hybrid Comparison Pseudocode

```
1 Input :  $A1, A2, A3$  — Coming from 3 IPs
2 Output :  $O$  — the result
3 Define variables  $m1, m2, m3$  and  $m4$ 
4 Set  $num\_bits$  as the total no of bits in the input
5 Set  $half\_bits$  as  $num\_bits/2$ 
6 for  $i = half\_bits$  to  $num\_bits$  do
7   |  $count =$  No. of 1's in  $A1[i], A2[i]$  and  $A3[i]$ 
8   | if  $count \geq 2$  then
9     |  $m1[i] = 1;$ 
10  | else
11  |   |  $m1[i] = 0;$ 
12  | end
13 end
14 for  $i = 1 : half\ bits$  do
15  | if  $A1[i] \geq A2[i]$  then
16  |   |  $m2[i] = A2[i]$  —  $m2$  being the smaller result;
17  |   |  $m3[i] = A1[i];$ 
18  | else
19  |   |  $m2[i] = A1[i];$ 
20  |   |  $m3[i] = A2[i];$  —  $m3$  is larger of the two inputs
21  | end
22  | if  $m2[i] > A3[i]$  then
23  |   |  $m4[i] = m2[i];$ 
24  | else
25  |   | if  $m3[i] > A3[i]$  then
26  |     |  $m4[i] = A3[i];$ 
27  |     | else
28  |     |   |  $m4[i] = m3[i];$ 
29  |     | end
30  | end
31 end
32  $O = \{m1, m4\};$  — Hardware Trojan free output
```

Chapter 4

Results and Discussion

The efficacy of the proposed PC technique and HC is validated by selecting different arithmetic units from [13] including add8_113, add8_174, mul8_320, mul8_375, mul8_496 and mul8_460. The Comparison, PC and HC are evaluated. The area and power of the proposed PC and HC are shown in the table ???. The table ??? shows that we achieve 40% reduction in Area and 50% power efficiency by applying our proposed techniques while effectively making the trojan.

4.1 Case Study

The two proposed designs so-called PC and HC are applied to a HT infected design to examine their efficacy. Three different infected designs (approximate multipliers) have been considered (The insertion of HT in a design is out of scope of this work; therefore, the attack model of [10] has been used to implanted a HT in three approximate multiplier designs which includes mul8_006, mul8_118, and mul8_132 respectively). These three approximate designs with planted HT are applied to an image enhancement application (IEA). . The all three HT infected multipliers when used individually for IEA result in a distorted output image as shown in Figure 4.1 (a), (b) and (c). Therefore, it is evident that the use of single approximate multiplier with HT inserted cannot be effectively used for IEA. However, there is an alternative to address this problem as stated in Section II-A. The effect of HT can be effectively masked by considering multiple approximate designs and applying a suitable mitigation technique. In our case, three approximate designs (with different level of HTs) are taken as input. The proposed PC and HC techniques mitigate the HT effect and provides a clear enhanced image in output as shown in Figure 4.1 (d) and (e). It can be observed clearly that the HT can modify the single multiplier employed to adjust the intensity of pixel values resulting in a distorted output. However, when PC and HC are applied to the three multipliers with HTs, the effects of the HTs are eliminated because even when one of

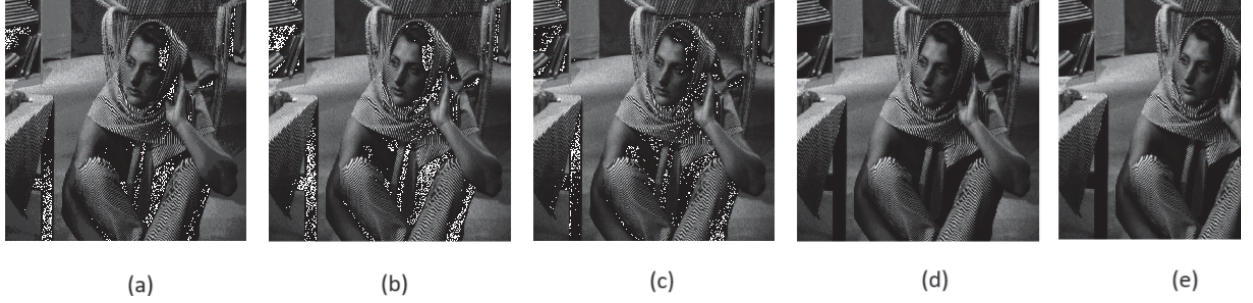


Figure 4.1: Outcomes of an image enhancement for three approximate multipliers with different Hardware Trojans inserted, (a) the trigger condition of the hardware Trojan is 1×1 and the payload logic is to force the result to be 255, (b) the trigger condition of the hardware Trojan is 1×2 and the payload logic is to force the result to be 255, (c) the trigger condition of the hardware Trojan is 1×3 and the payload logic is to force the result to be 255, and (d) the image enhancement result of the approximate multiplier using the proposed partial comparison-based method (e) the image enhancement result of the approximate multiplier using the proposed Hybrid technique

the inputs meet trigger condition, the other two multipliers still produce the acceptable results for the input. Moreover, Peak Signal to Noise Ratio (PSNR) and Structural Index Similarity (SSIM) values were calculated by MATLAB to assess image quality of our image generated after masking the trojan. The results indicated high image quality with PSNR and SSIM values of 33dB and 0.92 respectively. In this way, PC and HC are effectively used to generate HT free output.

4.2 Hardware Performance Analysis

To assess the hardware effectiveness of the proposed PC and HC against Hardware Trojans in AC systems, approximate multipliers and adders with different approximate levels are chosen. The area consumption and power consumption are compared between the comparison method, PC and HC. A rigorous performance analysis was conducted using Synopsys DC Compiler at the 40nm node(1V,25°C). Table 4.1 shows the area and power comparison of these techniques for different arithmetic units. Each approximate unit has been replicated thrice to simulate three different vendors. Resource type pertains to the types of approximate units as mentioned in [17], along with their associated WCEs (Worst Case Error) provided in parentheses. In our analysis, the Partial Comparison and Hybrid Techniques exhibited a remarkable reduction in area overhead(30%) compared to the traditional Comparison-Based Technique. PC and HC are more resource efficient because only a subset of bits are considered for compari-

Table 4.1. Area and Power of proposed Partial Comparison and Hybrid Techniques with Different Approximation Levels against Comparison based Method

8x8 Approximate Arithmetic Unit with Comparison Based Method		8x8 Approximate Arithmetic Unit with PC Based Method		8x8 Approximate Arithmetic Unit with Hybrid Based Method		Resource Type (WCE)
Area (um ²)	Power (mW)	Area (um ²)	Power (mW)	Area (um ²)	Power (mW)	
1344.873	0.4110	1270.609	0.3687	1258.967	0.3646	mul8_320(6)
1382.447	0.4478	1308.182	0.4040	1296.540	0.3999	mul8_375(32)
1284.545	0.3985	1210.280	0.3511	1198.638	0.3454	mul8_496(61)
1230.566	0.3919	1156.302	0.3428	1144.659	0.3384	mul8_460(121)
190.865	0.0411	133.711	0.0254	131.594	0.0185	add8_334(16)
241.668	0.0496	184.514	0.0339	182.397	0.0269	add8_419(25)

son which reduces computational workload compared to a full bit by bit comparison. HC simplifies decision making process for certain bits leading to resource and power efficient implementation. PC allows parallel processing of fewer bits which results in reduced power consumption as compared to bit by bit comparison. The proposed techniques maintain a delicate balance between maintaining accuracy in critical parts of computation and exploiting resilience of AC in relatively less critical regions. The results underscored the potential of these techniques to bolster security without compromising the fundamental goal of Approximate Computing i.e. minimizing resource utilization.

Power efficiency is another important metric, especially in applications where energy consumption is a critical concern. Our analysis revealed that both the Partial Comparison and Hybrid Techniques demonstrated a notable reduction in power consumption of (55%) compared to the Comparison-Based Technique. These findings affirm the compatibility of the proposed techniques with the energy-efficient objectives of AC systems.

The performance analysis was conducted using Synopsys DC Compiler at the 40nm node, a widely adopted technology in modern integrated circuit design. This choice ensures the relevance and applicability of our findings to real-world scenarios, emphasizing the practicality of implementing the proposed security techniques in modern day hardware environments.

Chapter 5

Conclusion

In recent years the AC paradigm has addressed the need of high computational efficiency for error-tolerant applications; however, a critical aspect neglected so far are the security implications when third-party approximate IPs are used in to accelerate the system design process. This paper marks a pioneering effort in addressing this neglected frontier by proposing two innovative techniques so-called the Partial Comparison (PC) and the Hybrid Comparison (HC). These methodologies, designed explicitly for AC systems, not only enhance security but also are resource-efficient compared to existing technique, attaining 30% and 55% improvement in area and power efficiency with a PSNR and SSIM of 33dB and 0.92 respectively. The AC takes center stage in modern computational paradigm, this paper serves as a foundation to refocus our attention on the security aspects that accompany the integration of third-party approximate IPs in any system. The proposed PC and HC offer not just a response to a long neglected challenge but a pathway to secure, efficient, and resilient AC systems.

Bibliography

- [1] F. L. Weiqiang Liu and M. Shult, “A retrospective and prospective view of approximate computing,” pp. 1–6, 2020.
- [2] G. M. S. Hany A.M. Amin a, Yousra Alkabani, “System-level protection and hardware trojan detection using weighted voting,” pp. 1–7, 2017.
- [3] C. W. Yuqin Dou, Chongyan Gu and W. Liu, “A novel method against hardware trojans in approximate circuits,” pp. 1–6, 2023.
- [4] C. A. Francesco Regazzoni and I. Polian, “Security: The dark side of approximate computing?” pp. 1–6, 2018.
- [5] N. B. Pruthvy Yellu, Michel A. Kinsy and Q. Yu, “Security threats in approximate computing systems,” pp. 1–6, 2019.
- [6] J. Han and M. Orshansky, “Approximate computing: An emerging paradigm for energy-efficient design,” pp. 1–6, 2013.
- [7] N. S. K. Qiang Xu and T. Mytkowicz, “Approximate computing: a survey,” pp. 1–15, 2015.
- [8] M. O. WEIQIANG LIU and P. MONTUSCHI, “Security in approximate computing and approximate computing for security: challenges and opportunities,” pp. 1–18, 2020.
- [9] C. P. Luca Collini, Benjamin Tan and R. Karri, “Reconfigurable logic for hardware ip protection: Opportunities and challenges,” pp. 1–7, 2022.
- [10] C. G. M. O. C. W. Yuqin Dou, Shichao Yu and W. Liu, “Security analysis of hardware trojans on approximate systems,” pp. 1–6, 2020.
- [11] N. R. S. Rajmohan and N. Naganathan, “Hybrid evolutionary design space exploration algorithm with defence against third party ip vulnerabilities,” pp. 2602—2614, 2020.

- [12] B. H. M. Beaumont and T. Newby, "Safer path: Security architecture using fragmented execution and replication for protection against trojaned hardware," p. 1000–1005, 2012.
- [13] Z. V. Vojtech Mrazek, Radek Hrbacek and L. Sekanina, "Evoapprox8b: Library of approximate adders and multipliers for circuit design and benchmarking of approximation methods," pp. 1–4, 2017.