EMPLOYING REDUNDANCY BASED TECHNIQUES TO PROVIDE RELIABILITY, SECURITY AND ACCOUNTABILITY IN MODERN PROCESSORS

RAJSHEKAR K

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY DELHI
SEPTEMBER 2017

EMPLOYING REDUNDANCY BASED TECHNIQUES TO PROVIDE RELIABILITY, SECURITY AND ACCOUNTABILITY IN MODERN PROCESSORS

by

RAJSHEKAR K

Department of Computer Science and Engineering

Submitted

in fulfillment of the requirements of the degree of **Doctor of Philosophy**

to the

Indian Institute of Technology Delhi

SEPTEMBER 2017

Certificate

This is to certify that the thesis titled **EMPLOYING REDUNDANCY BASED TECHNIQUES TO PROVIDE RELIABILITY, SECURITY AND ACCOUNTABILITY IN MODERN PROCESSORS** being submitted by **Mr. RAJSHEKAR K** for the award of **Doctor of Philosophy** in **Computer Science and Engineering** is a record of bona fide work carried out by him under my guidance and supervision at the **Department of Computer Science and Engineering, Indian Institute of Technology Delhi**. The work presented in this thesis has not been submitted elsewhere, either in part or full, for the award of any other degree or diploma.

Smruti Ranjan Sarangi
Assistant Professor
Department of Computer Science and Engineering
Indian Institute of Technology Delhi
New Delhi- 110016

Acknowledgements

I firstly thank my advisor, Dr. Smruti Sarangi, for all his help and guidance. He made me believe five years ago that I could be a PhD scholar, and he has now made me believe that I can advise PhD scholars myself. Thank you Sir.

I thank all the faculty in the Architecture group – Prof. Balakrishnan, Prof. Anshul Kumar, Prof. Panda and Dr Kolin Paul – and Dr. Shouri Chatterjee from the Department of Electrical Engineering, for reviewing my work and providing valuable insights.

I thank all my friends here at IITD for all the technical discussions that aided my research and deepened my understanding, as well as for all the other experiences that made life enjoyable and thought-provoking.

I thank all the boys back home for always being there. It made all the difference.

I thank all the boys from BMSCE for their support and encouragement. I got into IITD because of you guys!

I thank my parents for all their support and understanding, and for the sacrifices they have made the last seven and a half years I have been away from home.

I thank God, for all and everything.

Rajshekar K

Abstract

Though the classical goals in processor design – performance, power and area – are still being actively pursued, various new areas such as reliability and security have come into prominence.

As the transistors have become smaller, the threat of soft errors has increased. Mission critical systems are forced to employ chips fabricated at technology nodes that are at least 2-4 generations older, thereby suffering from low performance [1].

Moreover, as computers have become ubiquitous, attacking the computing infrastructure of an organization has emerged as a new form of aggression [2]. Commodity ICs are inexpensive; however, they do not provide any security guarantees whatsoever. Such ICs can potentially have malicious circuitry, popularly known as "Hardware Trojans". These can effectively bring down the computing infrastructure from the inside.

To further compound the problem, modern systems-on-chips (SOCs) have components designed by different design houses. Although the advantages of this paradigm are many, the provision of accountability is an emerging problem. The chip may fail to perform as expected on field. In such a scenario, perfect accountability – knowing which of the on-chip components are responsible – is desired. Such an accountability solution must be fair to all parties concerned, as being held responsible for a design/security flaw is detrimental to the design house's credibility in the market.

In this thesis, we apply the principle of redundancy to solve all of the above three problems, which are from three seemingly different domains – reliability, security and accountability. Redundancy is an attractive option because of its generality. The schemes developed are not application or hardware specific. Also, transistors have become cheaper. From costing a few dollars in 1955, the cost of a single transistor has dropped to around a billionth of a dollar in 2014 [3]. The investment made in redundancy is therefore not a big drain on the finances of an organization. The achieved gains far outweigh the costs.

संक्षेप

हालांकि प्रोसेसर डिज़ाइन में पारम्परिक लक्ष्यों जैसे कि, प्रदर्शन, ऊर्जा और क्षेत्रफल, को अभी भी सक्रिय रूप से शोध किया जा रहा है, विश्वसनीयता और सुरक्षा जैसे नए नए क्षेत्रों में भी प्रमुखता आई है।

जैसे जैसे ट्रांजिस्टर छोटे हो गए हैं, नरम त्रुटियों का खतरा बढ़ गया है। विशेष कार्य वाले सिस्टम जो कि कम से कम २-४ पीढ़ी पुरानी चिप्स को उपयोग करने के लिए प्रतिबंधित हैं, और इस कारण कम प्रदर्शन से पीड़ित हैं [१]।

इसके अलावा, कंप्यूटर सर्वव्यापी बन गए हैं, एक संगठन के कंप्यूटिंग अवसंरचना पर हमला करने का एक नया रूप आक्रमकता के रूप में उभरा है [२]। कमोडिटी आईसीएस सस्ती हैं, हालांकि, वे सुरक्षा गारंटी प्रदान नहीं करती हैं। इस तरह के आईसी संभावित रूप से दुर्भावनापूर्ण सर्किटरी हो सकती हैं, जिसे "हार्डवेयर ट्रोजन्स" के रूप में जाना जाता है। ये कंप्यूटिंग ढांचे पर बुरा प्रभाव डालते हैं।

समस्या को और अधिक जटिल बनाने हेतु, आधुनिक सिस्टम-ऑन-चिप्स (एसओसीएस) को विभिन्न रचना घरों द्वारा रचित किया जाता है। हालांकि इस प्रतिमान के कई लाभ भी हैं, परन्तु जवाबदेही का प्रावधान एक उभरती हुई समस्या है। फ़ील्ड पर अपेक्षा के अनुसार चिप निष्पादित करने में विफल हो सकता है। सही जवाबदेही वांछित है। हम यह जानना चाहते हैं कि कौनसा ऑन-चिप घटक जिम्मेदार है। इस तरह का एक जवाबदेही समाधान सभी दलों के लिए उचित होना चाहिए।

इस शोध-प्रबंध में हम उपरोक्त तीन समस्याओं को हल करने के लिए अतिरेक के सिद्धांत को लागू करते हैं, जो तीन अलग-अलग ज्ञानक्षेत्र से प्रतीत होते हैं - विश्वसनीयता, सुरक्षा और जवाबदेही। अपनी व्यापकता के कारण अतिरेकता एक आकर्षक विकल्प है। विकसित योजनाएं एप्लिकेशन या हार्डवेयर विशिष्ट नहीं हैं। साथ ही ट्रांजिस्टर सस्ते हो गए हैं। १९५५ में कुछ डॉलर की लागत से, एक ट्रांजिस्टर की लागत २०१४ में डॉलर के एक अरब हिस्से के करीब आ गई है [३]। अतिरेक में किया गया निवेश एक संगठन के वित्त पर भारी प्रभाव नहीं डाल रहा है। प्राप्त लाभ लागत से अधिक है।

Contents

List of Figures

List of Tables