



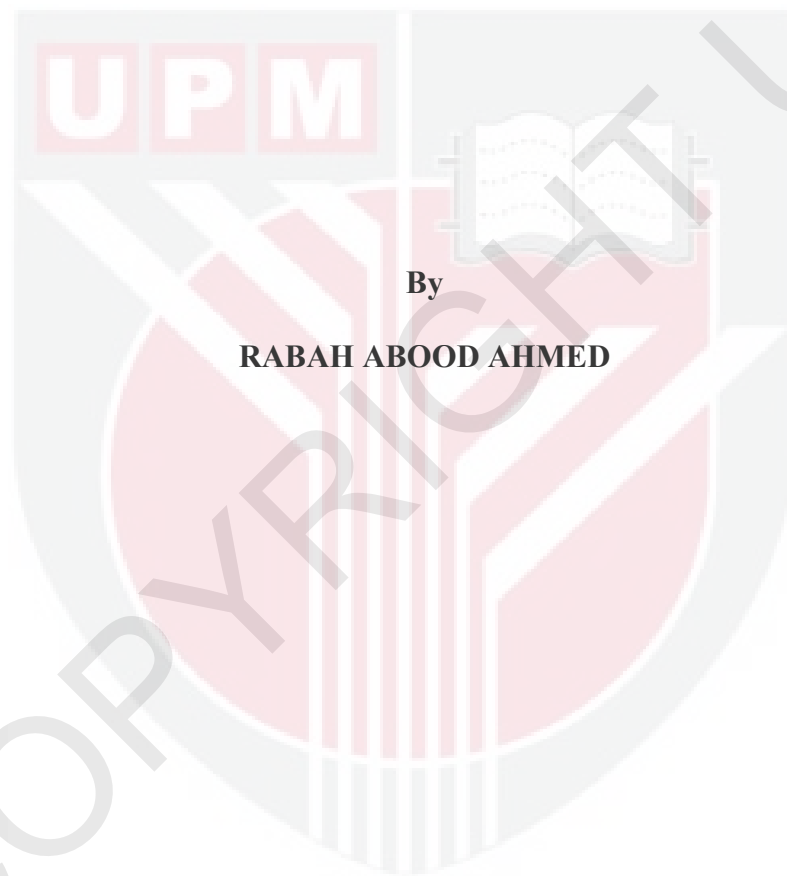
**UNIVERSITI PUTRA MALAYSIA**

***FAULT TOLERANCE OF L1 DATA CACHE MEMORY INDUCED BY  
INTRINSIC PARAMETERS FLUCTUATION IN SUB 10nm UTB-SOI  
MOSFETs***

**RABAH ABOOD AHMED**

**FK 2013 116**

**FAULT TOLERANCE OF L1 DATA CACHE MEMORY INDUCED BY  
INTRINSIC PARAMETERS FLUCTUATION IN SUB 10nm UTB-SOI  
MOSFETs**



By

**RABAH ABOOD AHMED**

**Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia,  
in Fulfillment of the Requirements for the Degree of Doctor of Philosophy**

**February 2013**



**TO MY FAMILY**

© COPYRIGHT UPM

Abstract of thesis presented to the Senate of University Putra Malaysia in fulfillment of the requirement for the degree of Doctor of philosophy

**FAULT TOLERANCE OF L1 DATA CACHE MEMORY INDUCED BY  
INTRINSIC PARAMETERS FLUCTUATION IN SUB 10nm UTB-SOI  
MOSFETs**

**By**

**RABAH ABOOD AHMED**

**February 2013**

**Chair: Khairulmizam Samsudin, Ph.D.**

**Faculty: Engineering**

Currently, the development of models at higher level of abstractions (system-level) to be able to incorporate effects at lower levels of abstractions (process /transistor) is in demand. This thesis addresses issues to enabling computer system simulation model in the presence of cell failures in L1 data cache corresponding to the impact of Intrinsic Parameters Fluctuation (IPF). These time-independent transistor-level sources of variation are randomly characterized in nature. This makes it difficult for the designer to include IPF impact in the design plan to overcome. This computer model is vital to analyze and evaluate credibly the effectiveness of L1 cache fault tolerance techniques in controlling the implications of IPF cell failures on microprocessor reliability and yield.

The objectives of this thesis are (i) to devise a framework to simulate system-level environment in the presence of L1 data cache cell failures corresponding to the impact of IPF, (ii) to introduce an evaluation method for deduce the effectiveness of L1 cache fault tolerance techniques in handling the actual error pattern caused by IPF cell failures in computer system under test and workload conditions, and (iii) to

investigate the implications of L1 data cache faults induced by the individual and combined impact of IPF sources on reliability of a general-purpose microprocessor.

The case study of this thesis is the impact of cell failures in the data array of L1 data cache in Intel Strong ARM@SA-1110 microprocessor. The failure models are generated corresponding to the individual and combined impact of Random Discrete Dopants in the source/drain regions (RDD), Line Edge Roughness (LER) and Body Thickness Variation (BTV) as the main sources of IPF in next nanometre-scale Ultra-Thin Body Silicon-on Isolator (UTB-SOI) transistor generations on Six-Transistors Static Random Access memory (6T SRAM) cell stability. The L1 cache fault tolerance techniques evaluated are hardware redundancy, parity check, Hamming single error correction double error detection (SECDED), and Hamming triple error detection (TED).

It was found that the rate of read faulty cells will rapidly increase in 6T SRAM cache with continued scaling of UTB-SOI device beyond 10 nm gate length. L1 cache conventional fault tolerance techniques, i.e. hardware redundancy, parity check, and SECDED, might be able to hold the implications of IPF cell failures in L1 data cache based 7.5 nm and 5 nm UTB-SOI device, particularly when 6T SRAM is designed with cell ratio of two. However, the effectiveness of these techniques was found to be sensitive to the existence of any faulty word in cache. Hence, their immunity against any transient fault that might occur during system operation will significantly degrade. Experimental results showed that in L1 data cache based on 5 nm UTB-SOI device, hybrid hardware redundancy with TED would achieve 68.2 percent of microprocessor chip yield in applications tolerate 10 percent performance loss

bound. This indicates that employing these techniques in industry will assist to keep 6T SRAM cache scalability even with the increasing impact of IPF.



Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

**HAD TERIMA KEROSAKAN UNTUK MEMORI CACHE DATA L1 YANG  
TERARUH OLEH FLUKTUASI PARAMETER INTRINSIK DALAM  
UTB-SOI MOSFETs LEBIH KECIL DARIPADA 10nm**

Oleh

**RABAH ABOOD AHMED**

February 2013

**Pengerusi: Khairulmizam Samsudin, Ph.D.**

**Fakulti: Kejuruteraan**

Kini, pembangunan model pada peringkat pemisahan yang lebih tinggi (peringkat system) supaya boleh digabungkan dengan efek-efek kepada peringkat pemisahan yang lebih rendah (proses/transistor) mempunyai banyak permintaan. Banyak projek dan penyelidik menumpukan kajian mereka untuk mencapainya. Tesis ini menumpukan kepada isu-isu untuk membolehkan simulasi system computer dalam kehadiran kegagalan sel-sel cache data L1 berkaitan dengan impak dari Intrinsic Parameters Fluctuation (IPF). Sumber-sumber variasi pada peringkat transistor yang tidak bergantung kepada masa ini digambarkan secara rawak. Ini menyebabkan kesukaran bagi para pereka untuk menyingkirkan atau memasukkannya ke dalam perancangan rekabentuk untuk diatasi. Model computer ini adalah penting untuk menganalisa dan menilai dengan kredibel keberkesanan teknik had terima kegagalan cache L1 dalam mengawal implikasi-implikasi kegagalan sel IPF kepada keutuhan dan hasil mikropemproses.

Objektif-objektif tesis ini ialah; (i) untuk mereka sebuah rangka untuk mensimulasikan sekitaran peringkat system dengan kehadiran kegagalan data cache L1 berkaitan dengan impak kepada IPF, (ii) untuk memperkenalkan kaedah evaluasi untuk teknik had terima kegagalan cache L1 untuk menyimpulkan keberkesannya dalam mengendalikan corak ralat yang disebabkan oleh sel IPF yang gagal dalam system computer di bawah kondisi ujian dan bebanan kerja, (iii) untuk mengkaji implikasi-implikasi ke atas keutuhan mikropemproses serbaguna dengan cache data L1 teraruh dengan impak-impak individu dan kombinasi dari sumber-sumber Fluktuasi Parameter Intrinsik.

Kajian kes untuk tesis ini ialah impak kepada kegagalan sel dalam tatasusun data untuk cache data L1 di dalam mikropemproses Intel Strong ARM@SA-1110. Model-model kegagalan itu dijana berdasarkan kepada impak-impak individu dan kombinasi dari Random Discrete Dopants dalam kawasan sumber/susutan (RDD), Line Edge Roughness (LER) dan Body Thickness Variation (BTV) sebagai sumber utama IPF dalam skala nanometer seterusnya bagi generasi transistor (UTB-SOI) pada kestabilan sel 6T SRAM. Teknik had terima kegagalan cache L1 yang dinilai ialah lewahan perkakasan, semakan parity, SECDEC, dan TED.

Adalah didapati bahawa kadar sel pembacaan rosak akan naik dengan pantas dalam cache 6T SRAM dengan pengecilan berterusan peranti UTB-SOI melebihi panjang get 10nm. Implimentasi secara agresif teknik konvensional had terima kegagalan cache L1 iaitu lewahan perkakasan, semakan parity, dan SECDEC mungkin boleh membawa implikasi kepada kegagalan sel IPF dalam cache data LI berdasarkan 7.5nm dan 5nm peranti UTB-SOI, terutamanya apabila 6T SRAM dicipta dengan nisbah sel dua. Walaubagaimanapun, keberkesanan teknik-teknik ini adalah



sensitive kepada kehadiran apa sahaja kata yang salah dalam cache. Oleh sebab itu, keimunan mereka terhadap apa sahaja kesalahan sementara yang mungkin berlaku sewaktu operasi system akan berkurang dengan nyata sekali. Keputusan eksperimen menunjukkan bahawa cache data berdasarkan 5nm peranti UTB-SOI, kelewahan perkakasan hybrid dengan TED boleh mencapai 68.2 peratus dari mikropemproses hasil cip dalam aplikasi yang boleh menahan 10 peratus kehilangan prestasi. Ini menandakan bahawa menggunakan teknik-teknik dalam industri akan membantu untuk menyimpan 6T SRAM cache kebolehan untuk diskala walaupun dengan semakin meningkat kesan IPF.

## ACKNOWLEDGEMENTS

First of all, I would like to praise ALLAH (S.W.T) for all his unlimited favors.

I am taking this opportunity to express my sincere gratitude to my principal supervisor, **Dr. Khairulmizam Samsudin**. This thesis would not have been possible without his constant advice, encouragement and cooperation. The regular meetings and discussions therein were invaluable in the realization of this research work. I am extremely grateful to him for his guidance and timely support in preparing this thesis.

I would also like to deeply thank **Associate Prof. Dr. Abdul Rahman Ramli** and **Dr. Fakhrul Zaman Rokhani** for being my committee members. I also want to thank them for all those discussions, and for their brilliant comments and suggestions, thank you.

I would like to express my great thankfulness and deepest gratitude to **my family** to whom I owed everything in my life from birth to death.

**RABAH ABOOD AHMED**

I certify that a Thesis Examination Committee has met on 7<sup>th</sup> February 2013 to conduct the final examination of Rabah Abood Ahmed on his thesis entitled “**Fault Tolerance of L1 Data Cache Memory Under the Influence of Intrinsic Parameter Fluctuation in Sub 10nm UTB-SOI MOSFETs**” in accordance with Universities and University Colleges Act 1971 and the Constitution of the University Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Doctor of Philosophy.

Members of Examination Committee are as follows:

**Nor Kamariah Noordin, Ph.D.**

Professor  
Faculty of Engineering  
Universiti Putra Malaysia  
(Chairman)

**Roslina Binti Mohd Sidek, Ph.D.**

Associate Prof.  
Faculty of Engineering  
Universiti Putra Malaysia  
(Internal Examiner)

**Wan Azizun Binti Wan Adnan, Ph.D.**

Lecturer  
Faculty of Engineering  
Universiti Putra Malaysia  
(Internal Examiner)

**Wong Weng Fai, Ph.D.**

Associate Prof.  
Department of computer Science  
National University of Singapore  
(External Examiner)

---

**SEOW HENG FONG, PhD**

Professor and Deputy Dean  
School of Graduate Studies  
Universiti Putra Malaysia

Date:

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

**Khairulmizam Samsudin, PhD**

Senior Lecturer  
Faculty of Engineering  
Universiti Putra Malaysia  
(Chairman)

**Abdul Rahman Ramli, PhD**

Associate Professor  
Faculty of Engineering  
Universiti Putra Malaysia  
(Member)

**Fakhrul Zaman Rokhani, PhD**

Senior Lecturer  
Faculty of Engineering  
Universiti Putra Malaysia  
(Member)

---

**BUJANG BIN KIM HUAT, PhD**

Professor and Dean  
School of Graduate Studies  
Universiti Putra Malaysia

Date:

## DECLARATION

I declare that the thesis is my original work except for the quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at universiti Putra Malaysia or at any other institution.

---

**RABAH ABOOD AHMED**

Date: 7 February 2013



## TABLE OF CONTENT

	<b>Page</b>
<b>DEDICATION</b>	<b>ii</b>
<b>ABSTRACT</b>	<b>iii</b>
<b>ABSTRAK</b>	<b>vi</b>
<b>ACKNOWLEDGEMENTS</b>	<b>ix</b>
<b>APPROVAL</b>	<b>x</b>
<b>DECLARATION</b>	<b>xii</b>
<b>LIST OF TABLES</b>	<b>xv</b>
<b>LIST OF FIGURES</b>	<b>xvi</b>
<b>LIST OF ABBREVIATIONS</b>	<b>xix</b>
<b>CHAPTER</b>	
<b>1 INTRODUCTION</b>	<b>1</b>
1.1 Motivation	1
1.2 Aim and Objectives	6
1.3 Scope of the Study	9
1.4 Thesis Contributions	10
1.5 Thesis Outline	12
<b>2 LITERATURE REVIEW</b>	<b>16</b>
2.1 Introduction	16
2.2 Intrinsic Parameter Fluctuation (IPF)	18
2.2.1 Random Discrete Dopant	20
2.2.2 Body Thickness Variations	21
2.2.3 Line Edge Roughness	22
2.3 The Effects of IPF Sources on Cache Memory	23
2.3.1 SRAM Cell Scalability	23
2.3.2 Cache Robustness	27
2.4 Characterization and Evaluation of the Implications of IPF	29
2.4.1 Device level	29
2.4.2 Circuit level	30
2.4.3 System Level	31
2.5 IPF Mitigation Techniques	38
2.5.1 Defect Tolerance Techniques	40
2.5.2 Faults Tolerance techniques	41
2.5.3 Hybrid Tolerance Techniques	42
<b>3 MODELING SYSTEM-LEVEL WITH CACHE INDUCED BY IPF</b>	<b>44</b>
3.1 Introduction	44
3.2 Incorporation a System-Level Simulation with IPF Impact	46
3.2.1 System-level Environment Simulation	48
3.2.2 Modeling Cache Induced by IPF Sources	51
3.2.3 Faults Injection in the System-level	57

3.3	Cache Fault Tolerance Techniques	61
3.3.1	Hardware Redundancy	62
3.3.2	Parity Check	63
3.3.3	Error Correction Code	64
3.3.4	Triple Error Detection technique	67
3.4	Benchmark Selection	70
3.5	Summary	72
<b>4</b>	<b>EFFECTS OF IPF IN 6T SRAM CACHE BASED UTB-SOI</b>	<b>74</b>
4.1	Introduction	74
4.2	Cache Cell Failures	76
4.3	Finer ECC Word Size in Cache Induced IPF	79
4.4	Benchmarks Workload	81
4.5	Summary	83
<b>5</b>	<b>TOLERANCE CAPABILITY OF L1 DATA CACHE TECHNIQUES TO CONTROL THE IMPLICATIONS OF IPF SOURCES</b>	<b>85</b>
5.1	Hardware Redundancy	88
5.2	Parity Checking	91
5.3	Error Correction Code	92
5.3.1	Tolerance Capability	93
5.3.2	Performance	95
5.4	Triple Error Detection	99
5.4.1	Tolerance Capability	99
5.4.2	Performance	101
5.5	Cache with Hardware Redundancy and Fault Tolerance Techniques	104
5.5.1	Cache Combined Hardware Redundancy with ECC	107
5.5.2	Cache Combined Hardware Redundancy and TED	111
5.6	Yield Study	113
5.7	Summary	124
<b>6</b>	<b>CONCLUSION</b>	<b>127</b>
6.1	Suggestion for Future Work	132
	<b>REFERENCES</b>	<b>134</b>
	<b>BIODATA OF STUDENT</b>	<b>145</b>
	<b>LIST OF PUBLICATIONS</b>	<b>146</b>

## LIST OF TABLES

Table	Page
3.1 Virtual computer system specifications	49
3.2 L1 data cache configuration	51
3.3 Mechanism for read fault	54
3.4 Mechanism for write fault	54
3.5 Lookup table information describes each failure in cache data array	56
4.1 Probability of cell failures in cache based 10 nm, 7.5 nm and 5 nm UTB-SOI transistor introduced by the impact of each individual and combined of IPF sources, caches using cell ratio $\beta$ of one	78
4.2 Probability of cell failures results in caches based on 7.5nm and 5 nm UTB-SOI MOSFET device using cell ratio $\beta$ of two	79
4.3 Cache extra check bits imposed by different ECC word size	80
5.1 Percentage of PCKFB in 7.5 nm and 5 nm 8-Kbyte cache	91
5.2 Penalties imposed by ECC-L1-dcache operations	96



## LIST OF FIGURES

Figures	Page	
2.1	Scaling transistor towards atomistic feature. (a) MOSFET with continuous doping and smooth edges and interfaces. (b) Sketch of MOSFET feature of 20 nm corresponding to 22 nm technology node with random discrete dopants, rough interface, and line edge roughness. (c) Sketch of a 10 nm MOSFET shows that device truly becomes a molecules scale device. (Source: 19)	19
2.2	<i>Si/SiO<sub>2</sub></i> top and bottom interface roughness in transistor with 10 nm gate length. ( Source: 42)	22
2.3	Schematic diagram for 6T SRAM cell	24
2.4	Intel, the 2X 6T SRAM area scaling objective (Source: 34)	25
2.5	Mean value of static noise margin SNM as a function of cell ratio for 10 nm, 7.5 nm, and 5 nm UTB-SOI MOSFETs induced by all IPF. (Source: 39)	39
3.1	A framework for simulating computer system operation in the presence of Intrinsic Parameters Fluctuation.	47
3.2	A simplified block diagram of the virtual computer system implemented on SIMICS.	48
3.3	Faults injection scheme.	58
3.4	Flowchart of cache interface module.	60
3.5	Flowchart of error checking module.	61
3.6	Implementation of hardware redundancy technique.	63
3.7	Flowchart of Hamming ECC SECDED model.	66
3.8	Flowchart of Hamming TED FTT model.	69
4.1	A descriptive view to the numbers of read faulty cells located in 5 nm UTB-SOI cache caused by RDD source of fluctuation.	78
4.2	The FCW probability as a function of faulty cell number in 8-Kbyte cache result for different ECC word sizes.	80

4.3	ECC practice design factor $M$ as a function of hard faulty cell numbers in 8-Kbyte cache designed with different ECC word size.	81
4.4	Percentage of instructions initiated by each benchmark access L1-dcache during system simulation.	82
4.5	Stress trend applied by benchmarks on all L1-dcache area during system simulation.	83
5.1	Percentage of L1-dcache read transactions marked as FWT and RFT incurred due to the individual and the combined of all IPF sources in 7.5 nm and 5 nm UTB-SOI devices.	86
5.2	Percentage of L1-dcache error free read transactions in 7.5 nm, and 5 nm L1-dcache with cell ratio $\beta$ of one and 5nm with $\beta$ of two under the COMB source of IPF.	87
5.3	8-Kbyte cache recovery result with different percentage of redundant rows/columns in cache memory using (a) 7.5nm, (b) 5nm UTB-SOI cache with $\beta$ one; and (c) 5nm cache with $\beta$ two.	90
5.4	Fault tolerance improvement in 7.5nm SECDED L1-dcache induced by RDD, and COMB sources.	93
5.5	Fault tolerance improvement in 5nm SECDED L1-dcache induced by LER, RDD, and combined impact of all IPF sources.	94
5.6	Performance degradation measured based on (a) normalized miss rate and (b) CPU performance loss in ECC- L1-dcache using 7.5 nm and 5 nm UTB-SOI device.	98
5.7	The percent of the experimented L1-dcache induced by 5nm LER, RDD, and COMB sources of IPF that work reliably with employed TED FTT.	101
5.8	CPU Performance degradation in 5 nm and 7.5 nm L1-dcache using TED tolerance technique.	102
5.9	Normalized read miss in cache employ TED tolerance technique.	103
5.10	Normalized PCK and ECC FWs in 8-Kbyte cache with cell failure rate correspond to the induced by the impacts of (a) RDD, and (b) COMB sources of IPF in 7.5 nm gate length UTB-SOI as a result of introducing 5-50 percent of extra redundant area.	105

5.11	Normalized PCK and ECC FWs in 8-Kbyte cache with cell failure rate correspond to the induced by the impacts of (a) LER, (b) RDD, and (c) COMB sources of IPF in 5 nm gate length UTB-SOI as a result of introducing 5-50 percent of extra redundant area.	106
5.12	Fault tolerance capability in L1-dCache using 7.5nm UTB-SOI MOSFET device under the influence of RDD and COMB sources of IPF.	108
5.13	Fault tolerance capability in L1-dCache using 5nm UTB-SOI MOSFET device induced by LER, RDD, and COMB sources of IPF.	109
5.14	The average loss of CPU performance that incurred due the SECDDED contribution when combined with 10-50 percent of aggressive HW-Redundancy in 7.5 nm and 5 nm UTB-SOI L1-dCache.	111
5.14	The average losses in CPU performance that uses L1-dcache employs TED and different percentage of HW-R to control the corresponding cell failures of individual and combinational impact of IPF sources in 7.5 nm and 5 nm UTB-SOI devices.	113
5.16	Probability of reliable cache vs probability of read faulty cells in 8-Kbyte cache data array.	115
5.17	Yield vs. performance loss bound in CPU chip using 7.5 nm UTB-SOI L1-dcache employed HW-R and TED to mitigate (a) RDD and (b) COMB sources.	119
5.18	Yield vs. performance loss bound in CPU chip using 5 nm UTB-SOI L1-dcache employed HW-R and TED to mitigate (a) LER (b) RDD and (c) COMB sources.	121
5.19	A comparison between proposed and conventional method in evaluate microprocessor chip yield with L1-dcache under COMB impacts of IPF sources in 5 nm UTB-SOI device that integrate TED FTT and different percent of HW-R.	122
5.20	Yield of CPU chip using 5 nm UTB-SOI L1-dcache designed with $\beta$ of two and under the influence of COMB sources of IPF.	124

## LIST OF ABBREVIATIONS

$\beta$	Cell ratio
$\mu$	Mean value
$\sigma$	Standard Deviation
$efa$	Effectiveness factor of area
$efc$	Effectiveness factor of correction
$L$	Number of rows in cache data array
$M$	ECC practical design factor
$m$	The number of syndrome bits
$N$	Number of bit cells per FTT word
$N_{TR}$	The number of transistors in L1-dcache data array in a wafer area
$P(F\_Cell)$	Probability of faulty cell in cache
$P_{RC}$	Probability of reliable cache
$P_{Z\_Sy}$	Probability of the entire syndrome bits to be zero
$r$	Number of faulty bit cell in FTT word

# CHAPTER 1

## INTRODUCTION

### 1.1 Motivation

Semiconductor industry continues to shrink transistor dimensions for decades to gain more functions and performance, while maintaining the cost for a chip. According to Moore's Law [1], the number of components per chip doubles roughly every two years. This aggressive scaling process to the conventional device architecture such as bulk MOSFET is rapidly approaching fundamental physical limits. Short-channel effects, lack of performance, material limitations and technological difficulties are increasing challenges hindering conventional MOSFET from reaching the ultimate scale [2]. For instance, the required high-channel doping to control short-channel effects are ultimately tradeoff the device performance degradations and increase in threshold voltage variations.

In spite of high-k/metal gate technology introduction, the fabrication process of a conventional MOSFET device in nanometer dimensions (i.e. sub-10 nm physical gate length) poses difficulties in controlling device-to-device variations due to the increasing role of intrinsic parameters fluctuation (IPF). Random Discrete Dopant (RDD) [3, 4, 5, 6], Line Edge Roughness (LER) [7, 8, 9], and Oxide Thickness Variation (OTV) [10] are the most important sources of IPF in conventional MOSFET device [11]. These sources of variations are static and associated with the fundamental discreteness of charge and matter in ultra-small devices [12] and cannot be

removed by strictly controlled process steps or improved fabrication equipment [13].

Due to the difficulty in characterizing all IPF sources by any design parameter(s), it is expected to change the current predictable design approaches to approximations. In particular, the impact of RDD in conventional MOSFET's channel region was already predicted to become a barrier to achieve device ultimate scale [14, 3].

For the purpose of ensuring the continuity of Moore's Law, an alternative device is required to replace the conventional bulk MOSFET. Recently, the International Technology Roadmap for Semiconductors (ITRS) [15] presented a novel MOSFET device architecture for sustaining MOSFET devices to scale deeper in nanometer regions. Ultra-Thin Body Silicon-on-Insulator (UTB-SOI) MOSFET with its very low doping concentration in channel region will have inherent immunity against RDD sources of IPF, and offers a superior electrostatic integrity and better performance in comparison with the conventional MOSFET [16].

In ultra small UTB-SOI transistors, fluctuations in numbers and positions of the discrete dopant atoms in device source/drain regions have been found to be unavoidable source of IPF. Moreover, due to the fabrication process limits,

LER has introduced as another source of IPF. The roughness of device line edge effectively introduces variation in each device active channel length. In addition, the inherent  $\pm 1$  atomic layer roughness of the top and bottom  $Si/SiO_2$  interfaces will also contribute in introducing the body thickness variation (BTV) variability in each individual device active channel region. The resultant of the combined effects of RDD in source/drain region, LER, and BTV will exacerbate the electrical mismatch between the similar devices [17].

It has been experimentally demonstrated at the device and circuit level that with the continued scaling of MOSFET device, IPF will adversely affect digital circuits performance and functionality [18, 13]. Particular attention has been given to investigate the impact of IPF sources on Static Random Access Memory (SRAM) functionality [19, 20].

The six-transistor (6T) SRAM is the dominant SRAM architecture used in contemporary high performance microprocessors. As the minimum size transistors are used to minimize cell area, 6T SRAM becomes the most vulnerable to manufacturing-related variations and intrinsic parameters fluctuation impacts [21]. Particularly, IPF sources are expected to have the dominant adverse impact on 6T SRAM cell stability in comparison with other manufacturing-related variations [22]: Increasing the impact of IPF sources exacerbates the electrical mismatch between the neighboring transistors in cell. This mismatch would degrade cell stability and might cause cell failure. Consequently, a catastrophic number of cache cells are expected to become faulty.

The implications of IPF cell failures is expected to adversely affect the reliability of the corresponding 6T SRAM cache memories and eventually will affect microprocessor chip yield. This would enforces cache system designers to go beyond design plan to the post-silicon phase to ensure cache system dependability ( i.e reliability, error correction , and error detection). Modern processors have large specialized and multi-level cache memory; however, particular attention have been given toward L1 data cache as the most susceptible component to the impacts of IPF sources in cache memory system [23, 24].

As the process and technology to build the next generation devices and IC are very complex and still unavailable, several simulation methodology at circuit-level have been introduced to investigate the implications of IPF cell failures on 6T SRAM cache yield [25, 26, 13]. Approaches of circuit-level simulation are limited because it is only suitable to investigate a small part of the systems associated with a circuit block. Moreover, evaluation of IPF cell failures on cache chip yield must consider cache fault tolerance techniques in handling these failures - with accepted area and performance overhead. At circuit level, the evaluation process either depend on an outdated guidelines [27] that does not consider recent cache fault tolerance techniques, or they consider only the hardware side of the system without considering the interactions with software [28]. Adopting only one of these evaluations might not lead to the optimal design decision that could be very expensive in cost and time.



It is critically important to examine the implications of intrinsic parameter fluctuation at system-level - to understand and evaluate clearly the ability of system level techniques in handling the incurred failures [29]. Mainly, two methods have been used to model the implications of cache cell failures to system-level simulations. The first method is by modeling the physical presence of cell failures (failure model) in cache system [30, 31]. Although, this methodology evaluates based on system-level fault tolerance techniques, the yield evaluation process can be considered as an extension to that used by circuit-level approaches; since it only considers the probability of producing a cache chip with safe failures : tolerance techniques that can guarantee to handle all the failures. In case of evaluating a cache fault tolerance techniques with the capability of handling a limited ratio of unsafe failures, this method will be unable to capture the tolerance capability of these techniques.

For the second method, the faults incurred due to these failures (fault model) are used to evaluate the effectiveness of the tolerance techniques in handling the failures. The evaluation of this method depends on how this fault model is represented. One general approach is performed by integrating a pre-prepared fault models that was previously proven to be a representative for the general pattern of fault occurrence in system [32]. This approach is not credible to modeling the implications of IPF cell failures, since it did not represent the actual fault pattern incurred in a system under test and workload conditions. A credible IPF fault model requires to comprehensively capture system workload interactions with fault mechanism of each faulty cell in cache introduced by IPF.

In the near future, a decision to adopting UTB-SOI technology for scaling 6T SRAM cache memory to nanometer regime requires to take in consideration the effects of the increasing rate of cell failures in cache induced IPF sources. Thus, there is an urgent need for a computer-aided design tool capable to credibly evaluate the effectiveness of cache cell failure tolerance techniques to controlling the implications of this problem on cache reliability, and the tradeoff that imposed by these techniques on performance. Devise such a tool will be vital to enabling system designers and manufacturers to taking the optimal decision which save lot of efforts, time and money. Furthermore, this tool will help to accelerate the development process of fault tolerance techniques.

## **1.2 Aim and Objectives**

The major aim of this thesis is to investigate the system-level implications of 6T SRAM cell failures in L1 data cache induced by different sources of intrinsic parameter fluctuation in nanometer scale UTB-SOI on the general-purpose microprocessor reliability and yield. Therefore, the objectives of this thesis are:

1. Devise a framework to simulate system-level environment with 6T SRAM data array failures in L1 data cache corresponding to the impact of intrinsic parameters fluctuation.
2. Propose an evaluation method to L1 cache fault tolerance techniques to handle cell failures introduced by intrinsic parameters fluctuation.
3. Investigate the implications of L1 data cache faults induced by the

individual and combined impact of intrinsic parameter fluctuation sources in 10 nm, 7.5 nm, and 5 nm gate lengths UTB-SOI device on reliability and yield of a general-purpose microprocessor.

For the first objective, a framework was developed using virtual computer platform capable to simulate a computer system operation in the presence of IPF cell failure pattern in 6T SRAM L1 data cache memory. SIMICS [33], the full system simulator, is used to simulate this computer platform. By default, SIMICS as the instruction set simulator, does not provide the mechanism to inject the effects of device and circuit levels into the simulated computer platform. This led to an integral strategy built in the SIMICS environment accounts for the impact of IPF sources in the simulated platform. The extraction of the impacts of IPF sources on 6T SRAM cache is performed by adopting the experimental results from a prior circuit-level simulation work. These results are statically processed and modeled as a virtual chip that represents the failure models induced by IPF sources. This framework enabled the capturing of the interactions between IPF cell failures model and its implications on system reliability and performance. The credibility of modeling these implications is also related with system workload. Therefore, a set of general-purpose benchmarks is applied on the virtual computer platform to simulate workload of the general-purpose applications.

The most important results that this framework must provide is from evaluating the effectiveness of fault tolerance techniques to control the implications of IPF failures on cache reliability and yield. Conventional methods to evaluate L1 cache fault tolerance techniques do not take into account the failures interactions

with system software layer, This could lead to a pessimistic perception, where the likely and unlikely effects will take the same occurrence probability. More pragmatic perceptions can be obtained by generating cell failures model based on the functional characteristics of the vulnerable 6T SRAM that captures IPF impacts at the lower level of abstraction (transistor-level). The derived faults will then be propagate up through system-level. Therefore, the second objective led to the introduction of a methodology specifically tailored to capture the effectiveness of L1 cache fault tolerance techniques which includes the software operation nature. Based on this methodology, fault tolerance techniques often used at L1 cache are modeled in the framework in such a way that can be introduced individually or in hybrid. These models provide statistics aggregated during system operation that helps to demonstrate in detail the ability of these techniques to maintain the reliability of the system and the imposed sacrifices in performance. This developed framework became a tool to estimate the margin of IPF sources impacts in nano-scale UTB-SOI device on system reliability and yield. Moreover, the reproducible experiments used in this methodology can assist the designer and developer of the fault tolerance techniques to understand in detail their effectiveness limits, which helps to develop these techniques faster.

© In the proposed framework for evaluating fault tolerance mechanisms in the cache, there is a third objective which is investigating the implications of different sources of IPF in next generation UTB-SOI MOSFETs with channel lengths from 10 to 5 nm on the reliability and performance of the system. Particularly, the concentration on L1 data cache which is considered as the most sensitive

component in computer architecture to the sources of variations [23, 31]. The study of each source of IPF in UTB-SOI is critically important to help the researchers community to focus their efforts towards the most aggressive sources. Moreover, the comprehensive investigation of the combined impact of all IPF sources, since their impacts are simultaneous in 6T SRAM cell, will lead to understanding exactly the extent of the impact of this process-level phenomenon.

### 1.3 Scope of the Study

- This research only consider RDD, LER, BTV sources of IPF in (10, 7.5, and 5) nm gate length UTB SOI in room temperature conditions, and exclude any other intra or inter die source of variations.
- It is only considered the impact of IPF on 6T SRAM stability and its related failures (read, and write) in the data portion of the L1 data cache of general purpose microprocessor.
- The occurrence of soft error or dynamic error in cache during system operation has been excluded.
- This investigation does not take into account the extra circuitry to implement the tolerance techniques.

## 1.4 Thesis Contributions

This study has introduced many key contributions to the state of the art in computer system modeling and validation techniques. The main contributions are listed as follows:

- A technique to incorporate information of cell failure model induced by IPF sources into system-level simulator as a lookup file to describe in detail the position and type of each failure in cache data array. Although in this study the focus is towards cache data array, using this technique can be expanded to include other cache portions using 6T-SRAM array such as cache tag array, fault tolerance parity bits array, etc. Empirically, this technique has been found to be capable to characterize accurately IPF cell failure model to system-level simulator by keeping the LUPF size relatively small. This small size LUPF is enabled to fit inside the memory of the host machine that reduces the effects on system simulation speed.
- A scheme to inject the actual error pattern induced by cache cell failures dynamically into system-level environment. This scheme deduces error pattern via the fault mechanism of each failure and its interaction with real system workload. This fault injection scheme provides two simulation mode that help to analyze the implications of cell failures on cache fault tolerance. The normal mode invokes fault mechanisms and propagates the error(s) through cache transactions up to the system-level environment. Fault emulation mode would just emulate faults by invoking the handler of fault mechanisms without enabling the error injection into system-level.

This simulation mode allows targeted analysis that does not employ any cache fault tolerance policy.

- Using a practical design factor ( $M$ ) to estimate the finer word size of Hamming error correction code in a cache with high failure rate. This  $M$  factor estimates according to the improvement in the fault tolerance capability in cache and the extra parity bits imposed to implement this technique. It was demonstrated that 32-bit is the optimal word size for Hamming single error correction double error detection code in cache with cell failure rate corresponding to the impact of IPF sources in 7.5 nm and 5 nm gate length UTB-SOI device.
- An evaluation method to the effectiveness of fault tolerance techniques to cover the implications of cache cell failures on cache reliability. This method offers a high credible evaluation results because it is based on the actual error pattern incurred in the system. In this thesis, it was proven that the evaluation of cache reliability using fault tolerance techniques with high ability to handle faulty words with multi faulty bits (such as Hamming triple error detection technique) will not be accurate unless by using this method.
- A case study that demonstrates the simulation of the influence of IPF sources in L1 data cache based nanometer scale UTB-SOI MOSFETs on reliability and yield of general-purpose microprocessor and how the perceptions captured can indicate a more robust L1 cache fault tolerance technique.

## 1.5 Thesis Outline

Chapter 2 provides the literature review for different research areas covered in this thesis. The chapter starts by introducing the concept of intrinsic parameter fluctuation (IPF), the main sources of IPF in UTB-SOI device which include : random discrete dopants in device source/drain regions, body thickness variation, and line edge roughness. The next section of the chapter overviews the implications of IPF on 6T SRAM cell scalability, emphasizes on the effects on exacerbating the cell failure in cache system, as well as, the sensitivity of L1 data cache robustness to cell failures exacerbation. Then, it reviews the present methodologies which characterize the impacts of IPF at device-level and evaluate their implications on cache at circuit and system levels.

Chapter 3 focuses on implementing the proposed methodology to investigate the general-purpose system with L1 data cache induced by IPF. This chapter starts with describing in detail each part of the framework used to implement this methodology including simulation of system-level environment, modeling cache memory induced IPF sources and developing of a faults injection scheme. Next, the mechanisms employed to model L1 cache fault and defect tolerance techniques is presented. These models include hardware redundancy for the defect tolerance techniques and parity check, Hamming SECDED ECC and Hamming TED techniques for the fault tolerance techniques. The strategy of introducing the  $M$  factor proposed to determine the finest word size for optimal SECDED ECC tolerance capability with minimal cache area overhead is also discussed. The last part of this chapter introduces the well selected benchmarks to model system



daily workload on the framework. These benchmarks are selected to represent this thesis objective requirement in modeling the workload for a general-purpose applications.

Chapter 4 focuses on investigating and modeling the impact of different sources of IPF in the next generations UTB-SOI devices on cache memory. It begins with presenting the probability of cell failures in cache corresponding to the individual and combinational impact of IPF sources in UTB-SOI devices with gate length 10 nm, 7.5 nm, and 5 nm. These sources includes random discrete dopants, body thickness variation, and line edge roughness. These results are also provided for cache designed with cell ratio  $\beta$  of two. All these results are adopted to model the virtual chip of the L1 data cache that to be incorporated with the developed framework. Then, using SIMICS virtual computer platform, the stress of the workload applied by the selected benchmarks on L1 data cache area are evaluated. Finally, using the proposed  $M$  factor, the finest ECC word in L1 cache under the influence of IPF in 5 nm and 7.5 nm UTB-SOI MOSFETs are selected.

Chapter 5 investigates the capability of system level tolerance techniques employed in L1 cache memory to handle the implications of the cell failures induced by different sources of IPF in UTB-SOI with 7.5 nm and 5 nm physical gate length devices. This investigation started with describing the implications of the cell failures in cache data array that does not employ any fault tolerance policy. The conclusions provided here present the expected pattern of fault occurrence in L1 data cache induced by different sources of IPF in 10 nm, 7.5 nm and 5 nm

UTB-SOI MOSFETs. These sources are random discrete dopants, body thickness variation, and line edge roughness, as well as the combined impact of all these sources. The tolerance capability of hardware redundancy, parity check, SECDED ECC, and TED to keep L1 data cache function reliably under the stress of all the benchmarks workload is evaluated. This evaluation is for L1 data cache with cell failures corresponding to the impact of the effective sources of IPF in 7.5 nm and 5 nm UTB-SOI device. These sources are random discrete dopants in 7.5 nm UTB-SOI and for 5 nm UTB-SOI are random discrete dopants, and line edge roughness. The evaluation for the L1 data cache with cell failures induced by the combined of all IPF sources in 7.5 nm and 5 nm UTB-SOI are also provided. The conclusions provided concentrates on the tolerance capability and the imposed losses in CPU performance. Next, the comparison between combining of hardware redundancy with either parity check or SECDED ECC techniques in cache with cell failures induced by each effective sources of IPF in 5nm and 7.5 nm UTB-SOI device are presented. The results for the combined of all IPF sources in 7.5 nm and 5 nm are also provided. Then, this chapter investigates the tolerance capability and performance loss in L1 data cache employed hardware redundancy technique with either SECDED ECC or TED to reliably control the implications of IPF effective sources in 5 nm and 7.5 nm UTB-SOI devices. Finally, the conclusions based on the yield study that evaluates the ability of these tolerance techniques in handling the implications of the individual and combined sources of IPF are presented. The foregoing investigations was performed with cache designed with cell ratio  $\beta$  of two as well.

Chapter 6 concludes the findings of this research and suggests possible future work that can extend the opportunities of handling the effects of IPF in next generation MOSFETs microprocessors and systems.



## REFERENCES

- [1] Moore, G. E. (1998). Cramming more components onto integrated circuits. *Proceedings of the IEEE*, 86(1), 82–85.
- [2] Wong, H. S. P., and Philip, S. (2002). Beyond the conventional transistor. *IBM Journal of Research and Development*, 46(2-3), 133–168.
- [3] Hoeneisen, B., and Mead, C. (1972). Fundamental limitations in microelectronics—I. MOS technology. *Solid-State Electronics*, 15(7), 819–829.
- [4] Philip Wong, H. S., Taur, Y., & Frank, D. J. (1998). Discrete random dopant distribution effects in nanometer-scale MOSFETs. *Microelectronics and Reliability*, 38(9), 1447–1456.
- [5] Taur, Y., Buchanan, D. A., Chen, W., Frank, D. J., Ismail, K. E., Lo, S.-H., Sai-Halasz, G. A., et al. (1997). CMOS scaling into the nanometer regime. *Proceedings of the IEEE*, 85(4), 486–504.
- [6] Asenov, A., Brown, A. R., Davies, J. H., Kaya, S., and Slavcheva, G. (2003). Simulation of intrinsic parameter fluctuations in decananometer and nanometer-scale MOSFETs. *IEEE Transactions on Electron Devices*, 50(9), 1837–1852.
- [7] Asenov, A., Kaya, S., and Brown, A. R. (2003). Intrinsic parameter fluctuations in decananometer MOSFETs introduced by gate line edge roughness. *IEEE Transactions on Electron Devices*, 50(5), 1254–1260.
- [8] Hamadeh, E., Gunther, N. G., Niemann, D., and Rahman, M. (2006). Gate line edge roughness amplitude and frequency variation effects on intra die MOS device characteristics. *Solid State Electronics*, 50(6), 1156–1163.
- [9] Gogolides, E., Constantoudis, V., Patsis, G. P., and Tserepi, A. (2006). A review of line edge roughness and surface nanotexture resulting from patterning processes. *Microelectronic Engineering*, 83(4-9), 1067–1072.
- [10] Asenov, A., Kaya, S., and Davies, J. H. (2002). Intrinsic threshold voltage fluctuations in decanano MOSFETs due to local oxide thickness variations. *Electron Devices, IEEE Transactions on*, 49(1), 112–119.

- [11] Roy, G., Adamu-Lema, F., Brown, A., Roy, S., and Asenov, A. (2006). Intrinsic parameter fluctuations in conventional MOSFETs until the end of the ITRS: A statistical simulation study. *Journal of Physics: Conference Series* (Vol. 38, pp. 188–191).
- [12] Mizuno, T., Okumura, J., and Toriumi, A. (1994). Experimental study of threshold voltage fluctuation due to statistical variation of channel dopant number in MOSFET's. *IEEE Transactions on Electron Devices*, 41(11), 2216–2221.
- [13] Bowman, K. A., Tang, X., Eble, J. C., and Meindl, J. D. (2000). Impact of extrinsic and intrinsic parameter fluctuations on CMOS circuit performance. *IEEE Journal of Solid-State Circuits*, 35(8), 1186–1193.
- [14] Frank, D. J., and Taur, Y. (2002). Design considerations for CMOS near the limits of scaling. *Solid-State Electronics*, 46(3), 315–320.
- [15] ITRS. (2009). International Technology Roadmap for Semiconductors (Executive Summary.).
- [16] Takeuchi, K., Koh, R., and Mogami, T. (2001). A study of the threshold voltage variation for ultra-small bulk and SOI CMOS. *IEEE Transactions on Electron Devices*, 48(9), 1995–2001.
- [17] Samsudin, K., Adamu-Lema, F., Brown, A., Roy, S., and Asenov, A. (2007). Combined sources of intrinsic parameter fluctuations in sub-25nm generation UTB-SOI MOSFETs: A statistical simulation study. *Solid State Electronics*, 51(4), 611–616.
- [18] Bhavnagarwala, A., Kosonocky, S., Radens, C., Stawiasz, K., Mann, R., Ye, Q., and Chin, K. (2005). Fluctuation limits & scaling opportunities for CMOS SRAM cells. *IEEE International Electron Devices Meeting, 2005, IEDM Technical Digest* (pp. 659–662).
- [19] Asenov, A. (2010). Statistical Nano CMOS Variability and Its Impact on SRAM. *Extreme Statistics in Nanoscale Memory Design*, 17–49.
- [20] Cheng, B., Roy, S., Roy, G., Adamu-Lema, F., and Asenov, A. (2005). Impact of intrinsic parameter fluctuations in decanano MOSFETs on yield and functionality of SRAM cells. *Solid-State Electronics*, 49(5), 740–746.

- [21] Burnett, D., Erington, K., Subramanian, C., and Baker, K. (1994). Implications of fundamental threshold voltage variations for high-density SRAM and logic circuits. *Symposium on VLSI Technology*. (pp. 15–16).
- [22] Bhavnagarwala, A. J., Tang, X., and Meindl, J. D. (2001). The impact of intrinsic device fluctuations on CMOS SRAM cell stability. *IEEE journal of solid-state circuits*, 36(4), 658–665.
- [23] Liang, X., Canal, R., Wei, G. Y., and Brooks, D. (2007). Process variation tolerant 3T1D-based cache architectures. *Proceedings of the 40th Annual IEEE/ACM International Symposium on Microarchitecture* (pp. 15–26).
- [24] Agarwal, A., Paul, B., Mukhopadhyay, S., & Roy, K. (2005). Process variation in embedded memories: failure analysis and variation aware architecture. *IEEE Journal of Solid-State Circuits*, 40(9), 1804–1814.
- [25] Samsudin, K., Cheng, B., Brown, A. R., Roy, S., and Asenov, A. (2006). Integrating intrinsic parameter fluctuation description into BSIMSOI to forecast sub-15nm UTB SOI based 6T SRAM operation. *Solid State Electronics*, 50(1), 86–93.
- [26] Bhavnagarwala, A. ., Kapoor, A., and Meindl, J. (2000). Dynamic-threshold CMOS SRAM cells for fast, portable applications. *Proceedings of the 13th Annual IEEE International* (pp. 359–363).
- [27] Stolk, P. A., Tuinhout, H. P., Duffy, R., Augendre, E., Bellefroid, L. P., Bolt, M. J. B., Croon, J., et al. (2001). CMOS device optimization for mixed-signal technologies. *International Electron Devices Meeting, IEDM Technical Digest*. (pp. 1021–1024).
- [28] Mukhopadhyay, S., Mahmoodi-Meimand, H., and Roy, K. (2004). Modeling and estimation of failure probability due to parameter variations in nano-scale SRAMs for yield enhancement. *Symposium on VLSI Circuits. Digest of Technical Papers*. (pp. 64–67).
- [29] Narendra, S., De, V., and Wilson, R. (2002). Process Variation: Is It too Much to Handle? *International Symposium on Quality Electronic Design*, ( pp. 213).
- [30] Roberts, D., Kim, N. S., and Mudge, T. (2008). On-chip cache device scaling limits and effective fault repair techniques in future nanoscale technology. *Microprocessors and Microsystems*, 32(5-6), 244–253.

- [31] Agarwal, A., Paul, B., Mahmoodi, H., Datta, A., and Roy, K. (2005). A process-tolerant cache architecture for improved yield in nanoscale technologies. *IEEE Transactions on Very Large Scale Integration Systems*, 13(1), 27–38.
- [32] Huang, B., Rodriguez, M., Li, M., and Smidts, C. (2007). On the development of fault injection profiles. *Symposium on Reliability and Maintainability* .(pp. 226–231).
- [33] Magnusson, P. ., Christensson, M., Eskilson, J., Forsgren, D., Hallberg, G., Hogberg, J., Larsson, F., et al. (2002). Simics: A full system simulation platform. *Computer*, 35(2), 50–58.
- [34] Kuhn K. J, (2011), Moore’s crystal ball: Device physics and technology past the 15 nm generation, *Microelectronic Engineering*, 88(7), 1044-1049.
- [35] Luisier, M., Lundstrom, M., Antoniadis, D. A., & Bokor, J. (2011). Ultimate device scaling: Intrinsic performance comparisons of carbon-based, InGaAs, and Si field-effect transistors for 5 nm gate length. *IEEE International on Electron Devices Meeting (IEDM)*, (pp. 1121 –1124).
- [36] Kamsani N., B. Cheng, S. Roy, and A. Asenov, Impact of random dopant induced statistical variability on inverter switching trajectories and timing variability, *IEEE International Symposium on Circuits and Systems*, (pp. 577-580).
- [37] Asenov, A. (1998). Random dopant induced threshold voltage lowering and fluctuations in sub-0.1  $\mu\text{m}$  MOSFET’s: A 3-D "atomistic" simulation study. *IEEE Transactions on Electron Devices*, 45(12), 2505–2513.
- [38] Samsudin, K., Cheng, B., Brown, A. R., Roy, S., and Asenov, A. (2006). Sub-25nm UTB SOI SRAM cell under the influence of discrete random dopants. *Solid State Electronics*, 50(4), 660–667.
- [39] Samsudin, K. (2006). Impact Of Intrinsic Parameter Fluctuations In Ultrathin Body Silicon-On-Insulator Mosfet On 6-Transistor SRAM Cell. Phd Thesis, University of Glasgow.

- [40] Uchida, K., Watanabe, H., Kinoshita, A., Koga, J., Numata, T., and Takagi, S. (2002). Experimental study on carrier transport mechanism in ultrathin-body SOI nand p-MOSFETs with SOI thickness less than 5 nm. *International Electron Devices Meeting (IEDM)*. (pp. 47 – 50).
- [41] Tsutsui, G., Saitoh, M., Nagumo, T., and Hiramoto, T. (2005). Impact of SOI thickness fluctuation on threshold voltage variation in ultra-thin body SOI MOSFETs. *IEEE Transactions on Nanotechnology*, 4(3), 369 – 373.
- [42] Brown, A. R., Adamu-Lema, F., and Asenov, A. (2003). Intrinsic parameter fluctuations in nanometre scale thin-body SOI devices introduced by interface roughness. *Superlattices and Microstructures*, 34(3–6), 283–291.
- [43] Esseni, D., Abramo, A., Selmi, L., and Sangiorgi, E. (2003). Physically based modeling of low field electron mobility in ultrathin single- and double-gate SOI n-MOSFETs. *IEEE Transactions on Electron Devices*, 50(12), 2445 – 2455.
- [44] Pavlov, A., and Sachdev, M. (2008). *CMOS SRAM circuit design and parametric test in nano-scaled technologies: process-aware SRAM design and test*. Springer.
- [45] Meng, K., and Joseph, R. (2006). Process variation aware cache leakage management. *Proceedings of the International Symposium on Low power electronics and design* (pp. 262–267).
- [46] Wang, H., Miranda, M., Dehaene, W., Catthoor, F., and Maex, K. (2005). Systematic analysis of energy and delay impact of very deep submicron process variability effects in embedded SRAM modules. *Design, Proceedings of the Automation and Test in Europe*. 2(pp. 914 – 919).
- [47] Luo, S. C., and Chiou, L. Y. (2010). A sub-200-mV voltage-scalable SRAM with tolerance of access failure by self-activated bitline sensing. *IEEE Transactions on Circuits and Systems*, 57(6), 440–445.
- [48] Mariani, R., and Boschi, G. (2005). A system-level approach for embedded memory robustness. *Solid-state electronics*, 49(11), 1791–1798.
- [49] *Working definitions of robustness*. (2001). Santa Fe Institute.



- [50] Tang, X., De, V. K., and Meindl, J. D. (1997). Intrinsic MOSFET parameter fluctuations due to random dopant placement. *IEEE Transactions on Very Large Scale Integration Systems*, 5(4), 369–376.
- [51] Takeuchi, K., Tatsumi, T., and Furukawa, A. (1997). Channel engineering for the reduction of random-dopant-placement-induced threshold voltage fluctuation. *International Electron Devices Meeting*, (pp. 841–844).
- [52] Stolk, P. A., Widdershoven, F. P., and Klaassen, D. B. M. (1998). Modeling statistical dopant fluctuations in MOS transistors. *IEEE Transactions on Electron Devices*, 45(9), 1960–1971.
- [53] Alexander, C., Roy, G., and Asenov, A. (2008). Random-Dopant-Induced Drain Current Variation in Nano-MOSFETs: A Three-Dimensional Self-Consistent Monte Carlo Simulation Study Using “Ab Initio” Ionized Impurity Scattering. *IEEE Transactions on Electron Devices*, 55(11), 3251–3258.
- [54] Patel, K., Liu, T.-J. K., and Spanos, C. J. (2009). Gate Line Edge Roughness Model for Estimation of FinFET Performance Variability. *IEEE Transactions on Electron Devices*, 56(12), 3055–3063.
- [55] Cheng, B. ., Roy, S., Roy, G., and Asenov, A. (2003). Integrating ‘atomistic’, intrinsic parameter fluctuations into compact model circuit analysis. *Proceeding of the ESSDERC* (pp. 437–440).
- [56] Roy, G., Brown, A. R., Adamu-Lema, F., Roy, S., and Asenov, A. (2006). Simulation Study of Individual and Combined Sources of Intrinsic Parameter Fluctuations in Conventional Nano-MOSFETs. *IEEE Transactions on Electron Devices*, 53(12), 3063–3070.
- [57] O’uchi, S., Masahara, M., Sakamoto, K., Endo, K., Liu, Y., Matsukawa, T., Sekigawa, T., et al. (2007). Flex-pass-gate SRAM design for static noise margin enhancement using FinFET-based technology. *IEEE Custom Integrated Circuits Conference*, (pp. 33–36).
- [58] Yu, S., Zhao, Y., Du, G., Kang, J., Han, R., and Liu, X. (2009). The impact of line edge roughness on the stability of a FinFET SRAM. *Semiconductor Science and Technology*, 24(pp 025005).

- [59] Roelke G. IV. (2006), Fault and defect tolerant computer architectures: Reliable computing with unreliable devices. PhD thesis, USA Air force institute of technology.
- [60] Kurdahi, F. J., Eltawil, A. M., Park, Y. H., Kanj, R. N., and Nassif, S. R. (2006). System-level SRAM yield enhancement. *Proceedings of the 7th International Symposium on Quality Electronic Design* (pp. 179–184).
- [61] Tammaru, E., and Angell, J. (1967). Redundancy for LSI yield enhancement. *IEEE Journal of Solid-State Circuits*, 2(4), 172–182.
- [62] Chen, A. (1969). Redundancy in LSI memory array. *IEEE Journal of Solid-State Circuits*, 4(5), 291–293.
- [63] Schober, V., Paul, S., and Picot, O. (2001). Memory built-in self-repair using redundant words. *Proceedings of the International Test Conference* (pp. 995–1001).
- [64] Benso, A., Chiusano, S., Di Natale, G., and Prinetto, P. (2002). An on-line BIST RAM architecture with self-repair capabilities. *IEEE Transactions on Reliability*, 51(1), 123–128.
- [65] Koh, C. K., Wong, W. F., Chen, Y., and Li, H. (2009). The Salvage Cache: A fault-tolerant cache architecture for next-generation memory technologies. *IEEE International Conference on Computer Design, ICCD* (pp. 268–274).
- [66] Wilkerson, C., Gao, H., Alameldeen, A. R., Chishti, Z., Khellah, M., and Lu, S.-L. (2008). Trading off Cache Capacity for Reliability to Enable Low Voltage Operation. *SIGARCH Comput. Archit. News*, 36(3), 203–214.
- [67] Chishti, Z., Alameldeen, A. R., Wilkerson, C., Wu, W., and Lu, S.-L. (2009). Improving cache lifetime reliability at ultra-low voltages. *Proceedings of the 42nd Annual IEEE/ACM International Symposium on Microarchitecture* (pp. 89–99).
- [68] Kim, J., Hardavellas, N., Mai, K., Falsafi, B., and Hoe, J. (2007). Multi-bit error tolerant caches using two-dimensional error coding. *Proceedings of the 40th Annual IEEE/ACM International Symposium on Microarchitecture* (pp. 197–209).

- [69] Hung, L. D., Irie, H., Goshima, M., and Sakai, S. (2007). Utilization of SECDED for soft error and variation-induced defect tolerance in caches. *Conference & Exhibition of Design Automation & Test in Europe*. (pp. 1–6).
- [70] Spica, M., and Mak, T. M. (2004). Do we need anything more than single bit error correction (ECC)? *International Workshop on Memory Technology Design and Testing* (pp. 111 – 116).
- [72] Arlat, J., Aguera, M., Amat, L., Crouzet, Y., Fabre, J.-C., Laprie, J.-C., Martins, E., et al. (1990). Fault injection for dependability validation: a methodology and some applications. *IEEE Transactions on Software Engineering*, 16(2), 166–182.
- [73] Nakata, Y., Ito, Y., Sugure, Y., Oho, S., Takeuchi, Y., Okumura, S., Kawaguchi, H., et al. (2011). Model-based fault injection for failure effect analysis - Evaluation of dependable SRAM for vehicle control units. *41st International Conference on Dependable Systems and Networks Workshops* (pp. 91–96).
- [74] Park, C. H., Oh, M. H., Kang, H. S., and Kang, H. K. (2004). A 15 nm ultra-thin body SOI CMOS device with double raised source/drain for 90 nm analog applications. *ETRI journal*, 26(6), 575–582.
- [75] Chen, Q., Guha, A., and Roy, K. (2007). An accurate analytical snm modeling technique for srams based on butterworth filter function. *International Conference on VLSI Design, Held jointly with 6th International Conference on Embedded Systems, 20th* (pp. 615–620).
- [76] Chang, L., Fried, D. M., Hergenrother, J., Sleight, J. W., Dennard, R. H., Montoye, R. K., Sekaric, L., et al. (2005). Stable SRAM cell design for the 32 nm node and beyond. *Symposium on VLSI Technology*. (pp. 128–129).
- [77] Cheng, B., Roy, S., and Asenov, A. (2007). The scalability of 8T-SRAM cells under the influence of intrinsic parameter fluctuations. *37th European Solid State Device Research Conference*. (pp. 93–96).
- [78] Koh, C. K., Wong, W. F., Chen, Y., and Li, H. (2009). Tolerating process variations in large, set-associative caches: The buddy cache. *ACM Transactions on Architecture and Code Optimization (TACO)*, 6(2), 8.

- [79] Sadler, N. N., and Sorin, D. J. (2006). Choosing an error protection scheme for a microprocessors L1 data cache. *International Conference on Computer Design*.
- [80] Hamming, R. W. (1950). Error Detecting and Error Correcting Codes. *Bell System Technical Journal*, 26( 2), 147–160.
- [81] Stapper, C. ., Lee, H. S., and IBM, E. J. (1992). Synergistic fault-tolerance for memory chips. *IEEE Transactions on Computers*, 41(9), 1078–1087.
- [82] NetBSD, The netbsd project. <http://www.netbsd.org/ports/amd64/>.
- [83] Intel Corporation, (2000), Intel Strong ARM SA-1110 Microprocessor Developers Manual.
- [84] Wikipedia Std, List of Applications of ARM Cores, [http://www.wikipedia.org/wiki/List\\_of\\_applications\\_of\\_ARM\\_cores](http://www.wikipedia.org/wiki/List_of_applications_of_ARM_cores).
- [85] Pavlov, A., Sachdev, M., and Pineda de Gyvez, J. (2004). An SRAM weak cell fault model and a DFT technique with a programmable detection threshold. *Proceedings of the International Test Conference*, (pp. 1006–1015).
- [86] Fieler, P., Loverro Jr, N., Inc, M., and Austin, T. (1991). Defects tail off with six-sigma manufacturing. *IEEE Circuits and Devices Magazine*, 7(5), 18–20.
- [87] C. Shin, M. H. Cho, Y. Tsukamoto, B.-Y. Nguyen, C. Mazurê, B. Nikoli•, and T.-J. K. Liu. (2010). Performance and Area Scaling Benefits of FD-SOI Technology for 6-T SRAM Cells at the 22-nm Node. *IEEE Transactions on Electron Devices*, 57(6) 1301-1309.
- [88] Gurindar. S. S. (1989). Cache memory organization to enhance the yield of high performance VLSI processors, *IEEE TRANSACTIONS ON COMPUTERS*, 38(4) 484492, 1989.
- [89] AMD. (2013) BIOS and Kernel Developer's Guide For AMD Family 10h Processors.

- [90] Slayman, C. (2005). Cache and memory error detection, correction, and reduction techniques for terrestrial servers and workstations. *IEEE Transactions on Device and Materials Reliability*, 5(3), 397–404.
- [91] Schuster, S. E. (1978). Multiple word/bit line redundancy for semiconductor memories. *IEEE Journal of Solid-State Circuits*, 13(5), 698 – 703.
- [92] Yamagata, T., Sato, H., Fujita, K., Nishimura, Y., and Anami, K. (2002). A distributed globally replaceable redundancy scheme for sub-half-micron ULSI memories and beyond. *IEEE Journal of Solid-State Circuits*, 31(2), 195–201.
- [93] Shooman, M. L. (2002). *Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design*. NY, USA: John Wiley and Sons, Inc.
- [94] Chen, C., and Hsiao, M. Y. B. (1984). Error-correcting codes for semiconductor memory applications: A state-of-the-art review. *IBM Journal of Research and Development*, 28(2), 124–134.
- [95] MacKay, D. J. C. (2003). *Information theory, inference, and learning algorithms*. Cambridge Univ Pr.
- [96] Guthaus, M. R., Ringenberg, J. S., Ernst, D., Austin, T. M., Mudge, T., and Brown, R. B. (2001). MiBench: a free, commercially representative embedded benchmark suite WWC-4. *IEEE international workshop* (pp. 3–14).
- [97] Weicker, R. P. (1984). Dhrystone: a synthetic systems programming benchmark. *Communications of the ACM*, 27(10), 1013–1030.
- [98] Doris, B., Jeong, M., Kanarsky, T., Zhang, Y., and Roy, R. A. (2002). Extreme scaling with ultra-thin Si channel MOSFETs. *International Electron Devices Meeting*, 2(pp. 267 –270).
- [99] Liow, T. Y., Tan, K. M., Lee, R., Zhu, M., Tan, B. L.-H., Samudra, G. S., Balasubramanian, N., et al. (2008). 5 nm gate length Nanowire-FETs and planar UTB-FETs with pure germanium source/drain stressors and laser-free Melt-Enhanced Dopant (MeltED) diffusion and activation technique. *Symposium on VLSI Technology* (pp. 36 –37).
- [100] O'Connor, K. . (1995). A source sensing technique applied to SRAM cells. *IEEE Journal of Solid-State Circuits*, 30(4), 500–511.

- [101] Hsiao, M. Y. (1970). A class of optimal minimum odd-weight-column SEC-DED codes. *IBM Journal of Research and Development*, 14(4), 395–401.
- [102] Chen, C., and Hsiao, M. Y. B. (1984). Error-correcting codes for semiconductor memory applications: A state-of-the-art review. *IBM Journal of Research and Development*, 28(2), 124–134.
- [103] Wilhelm, R., Engblom, J., Ermedahl, A., Holsti, N., Thesing, S., Whalley, D., Bernat, G., et al. (2008). The worst-case execution-time problem—overview of methods and survey of tools. *ACM Transactions on Embedded Computing Systems*, 7(3), 1–53.
- [104] Wadsworth G. P. and Bryan J. G. (1960) *Introduction to Probability and Random Variables*. McGraw-Hill, New York.
- [105] Asenov, A., and Samsudin, K. (2007). Variability in Nanoscale UTB SOI Devices and its Impact on Circuits and Systems. In S. Hall, A. Nazarov, and V. Lysenko (Eds.), *Nanoscaled Semiconductor-on-Insulator Structures and Devices*, NATO Security through Science Series (Vol. 17, pp. 259–302). Springer Netherlands