

Computer Architecture and Design Methodologies

Series Editors

Anupam Chattopadhyay, Nanyang Technological University, Singapore, Singapore

Soumitra Kumar Nandy, Indian Institute of Science, Bangalore, India

Jürgen Teich, Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU),
Erlangen, Germany

Debdeep Mukhopadhyay, Indian Institute of Technology Kharagpur, Kharagpur,
West Bengal, India

Twilight zone of Moore's law is affecting computer architecture design like never before. The strongest impact on computer architecture is perhaps the move from uncore to multicore architectures, represented by commodity architectures like general purpose graphics processing units (gpgpus). Besides that, deep impact of application-specific constraints from emerging embedded applications is presenting designers with new, energy-efficient architectures like heterogeneous multi-core, accelerator-rich System-on-Chip (SoC). These effects together with the security, reliability, thermal and manufacturability challenges of nanoscale technologies are forcing computing platforms to move towards innovative solutions. Finally, the emergence of technologies beyond conventional charge-based computing has led to a series of radical new architectures and design methodologies.

The aim of this book series is to capture these diverse, emerging architectural innovations as well as the corresponding design methodologies. The scope covers the following.

- Heterogeneous multi-core SoC and their design methodology
- Domain-specific architectures and their design methodology
- Novel technology constraints, such as security, fault-tolerance and their impact on architecture design
- Novel technologies, such as resistive memory, and their impact on architecture design
- Extremely parallel architectures

More information about this series at <http://www.springer.com/series/15213>

Ayantika Chatterjee · Khin Mi Mi Aung

Fully Homomorphic Encryption in Real World Applications

 Springer

Ayantika Chatterjee
Indian Institute of Technology Kharagpur
Kharagpur, India

Khin Mi Mi Aung
Institute for Infocomm Research
A*STAR
Singapore, Singapore

ISSN 2367-3478 ISSN 2367-3486 (electronic)
Computer Architecture and Design Methodologies
ISBN 978-981-13-6392-4 ISBN 978-981-13-6393-1 (eBook)
<https://doi.org/10.1007/978-981-13-6393-1>

Library of Congress Control Number: 2019930570

© Springer Nature Singapore Pte Ltd. 2019

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd. The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Contents

1	Introduction	1
1.1	Homomorphic Encryption in Real Applications: Few Case Studies	3
1.2	Summary of This Book	6
	References	7
2	Literature Survey	9
2.1	FHE in Cloud Computing	9
2.2	Mathematical Background	10
2.2.1	Somewhat Homomorphic Encryption	12
2.3	Few Related Works	16
2.4	FHE in Practical Algorithms	18
2.5	Conclusion	18
	References	19
3	Sorting on Encrypted Data	23
3.1	FHE Comparison Based Sort	25
3.1.1	Homomorphic Form of Sorting	27
3.2	Sorting and Security	28
3.2.1	The CPA Indistinguishability Experiment	28
3.2.2	Why Comparison Based Sorting is Secured?	30
3.3	Partition Based Sorting with Index Encryption	31
3.3.1	Encrypted Array with Encrypted Index	32
3.3.2	Problems of Recursion on Encrypted Data	32
3.3.3	Quick Sort Using Encrypted Stack	34
3.3.4	Encrypted Quick Sort Implementation	36
3.4	Timing Requirement for Sorting Schemes on Encrypted Data	37
3.4.1	Performance Analysis of Different Operations	38
3.4.2	Further Reduction of Recrypt to Introduce Error	39

3.4.3	Encrypted Insertion Sort	42
3.5	Conclusion	45
	References	46
4	Translating Algorithms to Handle Fully Homomorphic Encrypted Data	49
4.1	Challenges of Executing Encrypted Programs	50
4.2	Encrypted Variants of Basic Operators	50
4.3	Encrypted Bitwise and Assignment Operators	52
4.4	Encrypted Arithmetic Operators	52
4.4.1	Encrypted Addition and Subtraction	52
4.4.2	Encrypted Multiplication	53
4.4.3	Encrypted Division	53
4.5	Encrypted Relational Operators	55
4.5.1	Encrypted Comparison Operation	55
4.5.2	Encrypted Less Than/Greater Than Operator (FHE_Grt and FHE_Less)	57
4.6	Loop Handling on Encrypted Operations	58
4.7	Encrypted Program Termination Using Interrupt	62
4.8	Recursion Handling with Encrypted Operations	64
4.8.1	Design of Encrypted Stack	65
4.9	Design of Encrypted Queue	65
4.10	Design of Encrypted Linked List	65
4.11	Conclusion	69
	References	70
5	Secure Database Handling	71
5.1	Security Issues in Cloud	72
5.2	Sate of the Art	72
5.3	Basic Operations for Database Handling and Their Encrypted Variants	76
5.3.1	INSERT and SELECT Operation	77
5.3.2	TOP	80
5.3.3	LIKE	82
5.3.4	ORDER BY	82
5.3.5	GROUP BY	82
5.4	Advanced SQL: Encrypted JOIN	83
5.5	SQL Injection on Encrypted Database	84
5.6	Conclusion	85
	References	85

- 6 FURISC: FHE Encrypted URISC Design** 87
 - 6.1 Existing Encrypted Processors 87
 - 6.1.1 Heroic: Partial Homomorphic Encrypted Processor 88
 - 6.2 Implementing Fully Homomorphic Encrypted Processor Using a Ultimate RISC Instruction. 90
 - 6.2.1 Justification of Encrypted Processor Along with Encrypted Data 91
 - 6.2.2 Why URISC Architecture in Connection to FHE 91
 - 6.2.3 Performance Based Challenge. 92
 - 6.3 Design Basics of FURISC. 94
 - 6.3.1 Design of FURISC 95
 - 6.3.2 Encrypted Memory Module 96
 - 6.3.3 Encrypted ALU Module. 97
 - 6.3.4 Overall Architecture. 98
 - 6.4 Comparison with MOVE Based URISC 99
 - 6.4.1 Performance Evaluation: SBN Versus Move FURISC 100
 - 6.5 FURISC Applied to Realize Encrypted Programs 101
 - 6.6 Results 105
 - 6.6.1 Drawback of FURISC 106
 - 6.7 FHE Processor Implementation Challenges. 107
 - 6.8 Utilizing Compression Technique for FHE Architecture 108
 - 6.8.1 Run Length Encoding 108
 - 6.8.2 Proposed Encoding Module 108
 - 6.8.3 Different Choices of Subsequence Length to Store in RAM 112
 - 6.9 Conclusion 113
 - References 114
- 7 Conclusion and Future Work** 117
 - References 118
- Appendix A: Lattice Based Cryptography** 119
- Appendix B: LWE Based FHE** 123
- Appendix C: GSW Based FHE Approach.** 127
- Appendix D: FHE Based Libraries in Literature** 131
- Appendix E: Attacks on SWHE and FHE** 135
- Appendix F: Examples of Homomorphic Real World Applications** 139