Reconfigurable Cryptographic Processor

Leibo Liu · Bo Wang · Shaojun Wei

Reconfigurable Cryptographic Processor

Science Press
Beijing

Springer

Leibo Liu
Institute of Microelectronics
Tsinghua University
Beijing
China

Shaojun Wei
Institute of Microelectronics
Tsinghua University
Beijing
China

Bo Wang
Institute of Microelectronics
Tsinghua University
Beijing
China

ISBN 978-981-10-8898-8 ISBN 978-981-10-8899-5 (eBook)
https://doi.org/10.1007/978-981-10-8899-5

Jointly published with Science Press, Beijing, China

The print edition is not for sale in China Mainland. Customers from China Mainland please order the print book from: Science Press.

Library of Congress Control Number: 2018936628

© Springer Nature Singapore Pte Ltd. and Science Press, Beijing 2018
This work is subject to copyright. All rights are reserved by the Publishers, 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 publishers, 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 publishers 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 publishers remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

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

Foreword

The reconfigurable cryptographic processor is one of the ideal hardware implementations for encryption and decryption algorithms. Compared with traditional cryptographic processors, the reconfigurable cryptographic processor can meet the requirements of cryptographic application for high security, high energy efficiency, and high flexibility. In terms of security, the function of the dynamically reconfigurable computing architecture is not determined by either the hardware or the software alone, but it is dynamically defined by both the software programming and the hardware programming. The reconfigurable computing architecture has the "blank chip" feature after the power supply is cut off. Therefore, it is difficult to obtain the cryptographic algorithms through invasive attacks. Meanwhile, the execution model of the dynamically reconfigurable computing architecture has specialization and is indeterministic and it is very difficult to conduct side-channel attacks on it such as power analysis attacks, fault attacks, and electromagnetic attacks through behavioral modeling. Therefore, the dynamically reconfigurable computing architecture has high security against physical attacks. In terms of performance and power consumption, the dynamically reconfigurable computing architecture performs operations mainly by using a spatially parallel method, which is very suitable for the feature of cryptographic algorithms, and its energy efficiency (i.e., performance per watt) is high. In terms of functional flexibility, the reconfigurable computing architecture can change its hardware functions at runtime to fit them for different cryptographic algorithms and execution modes, and it has excellent flexibility. With the constant development of physical attack means in recent years, even if the security of cryptographic algorithms is very good, the attacker can still steal key information by using invasive or noninvasive physical attacks on the bottom-level cryptographic processor. Because the reconfigurable cryptographic processor has the above-mentioned outstanding advantages in resisting physical attacks, it has gradually become a hot research direction of cryptographic chips and a lot of relevant achievements on it have been published at

the top conferences of the cryptographic field and in periodicals of the cryptographic field in recent years.

Traditional cryptographic processors are mainly the application-specific integrated circuits (ASICs) and the instruction set architecture processors (ISAPs). The ASIC has obvious disadvantages in security and flexibility. By reversely analyzing ASIC chips, attackers can crack the cryptographic algorithms by the circuit implementation and steal the secret information being processed. In addition, the ASIC chip can only implement the specific cryptographic algorithms and it almost has no functional flexibility. Therefore, it cannot meet the rapidly developing demands of applications. The ISAP also has some security problems. Because it is easy to model the execution process of the system, the ISAP is likely to suffer noninvasive side-channel attacks. Meanwhile, the energy efficiency of the ISAP has been unable to meet the demands of current practical applications. The reconfigurable cryptographic processor has solved these difficult problems very well, and it has gradually been applied in practice. Therefore, it is likely that the reconfigurable cryptographic processor will be both the research and application directions of the future cryptographic processor.

The research team headed by Prof. Leibo Liu, the author of the book, is one of the best domestic teams in the reconfigurable cryptographic processor research field because it has worked in the field for a long time and accumulated a lot of experiences. The Institute of Microelectronics, Tsinghua University, in which Dr. Liu works completed two key projects of the National 863 Program in the reconfigurable computing direction in the 11th and the 12th Five-Year Plan periods, and the institute was awarded a second-class prize of the 2015 National Technological Invention Award. Acting as a leader in the frontier research of the domestic reconfigurable computing field, the institute has published a series of influential academic papers at top-level meetings of the relevant fields and in relevant periodicals, published an academic monograph *Reconfigurable Computing*, obtained relevant patents, and won gold medal in the 2015 National Patent Award. The institute has conducted some fruitful pioneering research in the application of reconfigurable computing technology to the cryptographic field in recent years and proposed the key technologies for improving the security, flexibility, and energy efficiency of cryptographic processors by making use of the dynamic reconfigurable features, including fault attack countermeasures and electromagnetic attack countermeasures based on the dynamic reconfiguration with spatial and temporal randomization, technologies of generating physical unclonable functions by using reconfigurable architectures, and fault attack countermeasures by making use of the improved Benes network. The novelty, advancement, and effectiveness of these technologies have impressed me very much.

In this book, the description is precise, the materials are well-organized, the contents are novel, and the viewpoints are original. This book not only describes in detail the basic knowledge and current research status of cryptographic processors,

but also discusses the design methods and development direction of reconfigurable cryptographic processors. It is an extremely good monograph in the field. Therefore, I would love to recommend it to readers.

Beijing, China Jiren Cai

Preface

Reconfigurable cryptographic processor has special technological advantages in security, energy efficiency (performance per watt), and functional flexibility, compared with the other cryptographic processors such as instruction set architecture processors (ISAP), field-programmable gate arrays (FPGA), or application-specific integrated circuits (ASIC).

The first technological advantage is the advantage in the security of the cryptographic processor due to the following two reasons. Firstly, though the processing elements and interconnections of reconfigurable cryptographic processors may be heterogeneous, they are still very regular in terms of circuits as well as the placement and routing. It is difficult to obtain the information of the cryptographic algorithms by observing the hardware structure and circuit construction. Therefore, the information of cryptographic algorithms will not be leaked during the tape-out process or even after the chip is lost. This feature is called the "blank chip feature" of reconfigurable cryptographic processors, which is very concerned by a lot of users. Secondly, reconfigurable cryptographic processors have the features of dynamic reconfiguration and partial reconfiguration. The function of processing elements and the interconnection among them can be changed within several cycles. The reconfiguration time is from over 10 ns to dozens of nanoseconds (Note: The FPGA reconfiguration time is from several hundreds of milliseconds to several seconds). Therefore, its capability of physical attack resistance is far stronger than that of the traditional cryptographic processors, which is one of the reasons why the security of the reconfigurable cryptographic processor is high. The content of this part is one of the highlights of the book, and it will be described in detail.

The second technical advantage is that reconfigurable cryptographic processors have very high energy efficiency, while it can meet the functional flexibility demands for the diversification and constant evolution of cryptographic algorithms. This is mainly because the reconfigurable processor supports hardware programming as well as software programming, and it can meet the constantly changing software demands by dynamically changing hardware. As we all know, the energy efficiency of ASICs is the best. However, this type of circuits does not have any flexibility.

After the silicon implementation is finished, the functions cannot be changed and no new functions can be added to it unless it is redesigned and taped out again. Since now the chip research and development (R&D) costs are becoming increasingly high, such implementation mode that needs a lot of time and very high R&D costs will be gradually eliminated in the market. Cryptographic processors using the instruction set architecture are of the best functional flexibility. This type of cryptographic processors can be used to perform most of the cryptographic algorithms at present and even in future; however, its energy efficiency is very low. It can reach only $1/10^4$ of or even lower than the energy efficiency of the ASIC, which is far from meeting the application demands. In addition to the ASIC and the ISAP, there is a more common way to implement cryptographic processors, i.e., the way of using the programmable logic device. However, the performance of this implementation approach is still not ideal in energy efficiency and functional flexibility. The reasons for that can be explained in two aspects. Macroscopically speaking, the flexibility of programmable logic devices such as the FPGA are too flexible (Note: As long as the number of programmable units is large enough, digital logic in almost any form can be implemented), and the high flexibility is obtained at the cost of greatly reducing the energy efficiency and area efficiency (i.e., performance vs. area). Though cryptographic operation needs functional flexibility, it is not wise to obtain such high functional flexibility which is unnecessary and cannot be fully used by reducing the performance and increasing the power consumption and area consumption. Microscopically speaking, the programming granularity of programmable logic devices such as the FPGA is too fine (For example, the core processing element is the lookup table (LUT) of 1-bit granularity), which results in too much configuration information and too long configuration time, makes it impossible to implement dynamic and partial reconfiguration limiting the improvement of energy efficiency and area efficiency. Though some commercial FPGA advertisement claims that the product has such function, we do not think the FPGA can implement the same dynamic and partial reconfiguration as reconfigurable processors. This is determined by the architecture of FPGA. Cryptographic processors implemented in other types of technologies such as the system-on-a-chip (SoC), the system-on-a-programmable-chip (SoPC), the programmable system-on-a-chip (PSoC), and the application-specific instruction set processor (ASIP) are different combinations or variants of the above-mentioned three types. For example, a SoC is in fact a combination of an ISAP and an ASIC, while a SoPC is a combination of a programmable logic device and an ISAP and the ASIP is the customized ISAP for some specific fields. Though these cryptographic processors have inherited the advantages of ASICs, ISAPs, and the programmable logic devices, they have their inherent disadvantages. Therefore, their energy efficiency and functional flexibility are still not good enough and cannot be improved much in the future. Reconfigurable cryptographic processors are customized for cryptographic operations. Its functions can be dynamically reconfigured after silicon implementation. It is backward compatible with cryptographic algorithms. Its functional flexibility can meet the requirements for cryptographic algorithms, while its energy and area efficiencies are maintained with moderate flexibility. Our research results have shown that the

energy and area efficiencies of reconfigurable cryptographic processors can reach 1–3 orders of magnitude or even higher than those of the ISAP and the programmable logic device on condition that the flexibility demand of cryptographic algorithms is met. Why and how we obtained such results will be described and analyzed in detail in the book.

This book consists of seven chapters: Chap. 1 describes the state-of-the-art researches on cryptographic processors, analyzes the advantages and disadvantages of traditional ASIC and ISAP cryptographic processors in terms of performance, power consumption, flexibility, and security, introduces the reconfigurable computing concept and the cutting-edge researches on reconfigurable cryptographic processors. In Chap. 2, the current mainstream cryptographic algorithms are presented using the reconfigurable computing architecture as the implementation hardware platform. The extraction of common logics of cipher algorithms and the features of data types, and the analysis of the parallelism of algorithms are described. This chapter also preliminarily discusses the hardware architecture design based on the implementation of cipher algorithms. Chapter 3 analyzes the hardware architecture design of reconfigurable cryptographic processors in two aspects: the datapath and the controller. The design methods of hardware architecture for cryptographic algorithms are also proposed. Chapter 4 introduces the compilation process of reconfigurable computing processors, discusses the special optimization methods for cryptographic algorithms, and demonstrates with instances of the compilation of specific cryptographic algorithms. Chapter 5 describes a reconfigurable cryptographic processor chip designed by our team. It includes the basic architecture, the key technologies, the integrated development tool, and the comparisons with other state-of-the-art designs. Chapter 6 describes several novel physical attack countermeasures for reconfigurable cryptographic processors, including countermeasures against physical attacks using random reconfiguration and the computing resources in the reconfigurable array. Compared with the applying of traditional countermeasures to a reconfigurable architecture, these new countermeasures based on the reconfigurable features can reduce the performance loss, area consumption, and power consumption caused by the security improvement through resource reuse and it is possible that it can resist new attacks in the future. Chapter 7 discusses the development trends of the reconfigurable cryptographic processor technology and focuses on exploring the hardware Trojan and the fully homomorphic encryption.

This book has embodied the collective wisdom of the reconfigurable cryptographic processor research team at the Institute of Microelectronics, Tsinghua University, for the past seven to eight years. We are very grateful to our colleagues and some students such as Bo Wang, Jianfeng Zhu, Hai Huang, Neng Zhang, Ao Li, Zhouquan Zhou, Dongxing Wang, Chenchen Deng, and Hanning Wang for their contribution. We really appreciate the great support and guidance from Prof. Shaojun Wei. We are very grateful to academician Jiren Cai, a famous expert in the information security field of China. He has read the book and written a

preface though he was very busy at that time. Finally, I would like to thank my wife and children for their understanding. It is almost impossible for me to complete the work without their support, and they will be an important force that drives me forward and makes me continue to work hard in the future!

Beijing, China Leibo Liu

Contents