Computer Architecture and Design Methodologies

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 unicore 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 will cover 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

Sikhar Patranabis · Debdeep Mukhopadhyay
Editors

Fault Tolerant Architectures for Cryptography and Hardware Security

Springer

Editors
Sikhar Patranabis
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
Kharagpur, West Bengal
India

Debdeep Mukhopadhyay
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
Kharagpur, West Bengal
India

ISSN 2367-3478 ISSN 2367-3486 (electronic)
Computer Architecture and Design Methodologies
ISBN 978-981-10-1386-7 ISBN 978-981-10-1387-4 (eBook)
https://doi.org/10.1007/978-981-10-1387-4

Library of Congress Control Number: 2018932188

Printed on acid-free paper

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

Preface

When a secret is revealed, it is the fault of the man who confided it.

Faults can be catastrophic for cryptosystems! In most cases, even a single well-formed fault is sufficient to reveal secret keys of the underlying ciphers. Even mathematically strong ciphers like the Advanced Encryption Standard (AES), RSA, are all vulnerable against such *fault attacks*. On the other hand, to meet the real-time requirements cryptosystems are often implemented in hardware platforms (in the form of FPGAs, ASICs), and as highly optimized software libraries (like OpenSSL) to be executed on a wide range of processors. Reliability of such complex designs, both on hardware and software is a serious issue. The problem becomes even more challenging than a standard reliability problem due to the fact that the reliability issue does not only lead to a failure, but could lead to a complete collapse of the cryptosystems. Like all security problems, here also there are two entities: the fault attacker and a fault attack-resistant designer. The former tries to develop novel fault injection mechanisms, fault analysis techniques which impose less restrictions on the fault injection and are based on more practical and achievable fault models. On the other hand, the designers' role is to evaluate the applicability of classical fault tolerance techniques to mitigate these threats, and to augment the defenses by dedicated methodologies. The designers also need a thorough understanding of the fault models, and the exploitable fault space to develop safeguards, which are sufficient to thwart the attacks. For making the treatment complete, it is also necessary to understand the reliability issues in modern day processors, to comprehend the threats in triggering these menacing attacks. Finally, it is also desirable to develop automated tools to assist in the fault analysis process to unearth new fault attacks against the cryptosystems. This would indeed reduce design cycles and help designers in the long run to develop fault-resistant systems with lesser effort.

The book tries to cover all these aspects and present the reader with a one-stop platform to develop comprehensive knowledge in this research area. A brief topic wise summary of the book is provided underneath to help the reader foresee his journey through the book:

- **Fault Analysis Methods and Fault Models**: There are different types of fault analysis methods which have been developed, along with a wide variety of injection techniques. Knowledge of the various methods and capabilities help the attacker unearth practical attacks. Otherwise, there is always a chance of developing fault attacks which are not practical, and hence not useful!
- **Classical Fault Analysis of Public-Key and Symmetric-Key Ciphers**: Different variations of fault analysis have been developed on public- and symmetric- key ciphers. The most popular form of fault analysis is what is called as Differential Fault Analysis (DFA), which is a combination of Differential Cryptanalysis and faults. The book provides a background on DFA, starting with the classic attacks on RSA. However, more detailed treatment is provided on symmetric cipher standards, like AES, when the fault affects both the datapath and key schedule. The book also provides treatment of fault analysis of stream cipher standards, like Grain, with practical results to demonstrate how real-life faults manifest and can be exploited.
- **Combination of Side-Channel and Fault Analysis**: Fault Analysis has been inspired and supplemented by side-channel analysis. Combinations have led to powerful attack vectors, like Differential Fault Intensity Attacks (DFIA), which try to utilize the fact that the fault injections are not necessarily uniform, and thus leaves a bias. DFIA present a side channel akin to analysis methodology to exploit this bias. On the other hand, researchers have tried to combine side-channel leakage, through say power consumption, and perform subsequent fault analysis to develop very strong attacks on standard cryptosystems. In the book, we support the theory with accompanied case studies on AES and PRESENT like standard ciphers.
- **Laser-based Fault Injection Techniques**: Controllability of fault injection methods is central to the success of fault attacks. Lasers provide a unique capability to target fault injections with greater accuracy, but also requires proper processing of the device and also understanding of the fault model. The book presents case studies on AES and the recently popular stream cipher, called ChaCha, to show a new type of fault attack, namely Instruction Skip Attack and Instruction Replacement Attack.
- **Software-Triggered Fault Analysis: RowHammer Bugs**: Recent day (DRAM) memory chips manifest a reliability issue, reported as RowHammers, which shows bit flips in rows adjacent to those rows which are accessed faster than the refresh rates repeatedly. This bug seems to offer a mechanism of launching fault injections through software codes! The book provides a detailed case study on a 1024-bit RSA key-based ciphering using the standard GNU-MP big integer library. It shows that though difficult, it is indeed possible to perform bit flips in the secret keys, a single instance of which is enough to reveal the complete key due to the power of DFA.

- **Automation of Fault Analysis**: Though most of the fault analysis techniques on ciphers, like AES, had been developed like the conventional cryptanalysis community, of human observation and analysis, it is much coveted to develop automated tools in this direction. An overview of such an automated method, called as Algebraic Fault Analysis (AFA) is provided with case studies on PRESENT, is provided. Such techniques indeed may pave ways to future analysis and design tools to unearth new attacks without human intervention, and thus shorten design time and effort.
- **Classical Fault Tolerance**: Several approaches for mitigating the powerful DFA have been developed using classical fault tolerance techniques. These techniques, which are largely based on various forms of redundancy, need to be understood for performing trade-offs between performance and security versus fault analysis for cryptosystems.
- **Countering Biased Fault Attacks**: The difference between classical fault tolerance and fault attacks is the fault injection methodology. In classical fault tolerance, while it is widely assumed all faults are equally likely, in attacks like DFIA there is a bias in the injector. This can lead to the increase in the probability of fault collisions, and attacks against classical fault tolerance techniques. In this context, we propose a technique called Fault Space Transformation (FST), which can be used to counter this increase of fault collision probability by changing the fault space. This technique has been illustrated with experimental results on FST being applied to AES-128.
- **Infective Countermeasures**: While the previous mitigation techniques attempt to detect a fault injection by an explicit comparison step, there is another family of countermeasures which infects the differential by a value which is not related to the key. These techniques are called as Infective Countermeasures, which have been cryptanalyzed several times and are difficult to construct. In this chapter, we present an infective countermeasure for AES-128, and provide a formal analysis method to show the level of security against various fault models. Finally, we fortify the method against the instruction fault model on an x86 ISA, using the idea of idempotent instructions. However, the security comes with the cost of a significant performance overhead which is also discussed.
- **Reactive Countermeasures**: As mentioned, all the above countermeasures come with a significant cost. In this book, we develop a new class of countermeasures, which are largely reactive in nature. The principle is based on digital artefacts and sensors being deployed in the chip, to be alert against a fault injection. A detailed case study on such a design style has been furnished on AES with reports on fault injections. This method seems to provide a very low overhead method for thwarting fault attacks by eliminating them at source.

The book thus covers a wide range of topics on fault analysis of cryptosystems, and is aimed at catering to postgraduate students and practitioners in the area of Hardware Security. It can also be used in final year graduate courses, albeit leaving

out few chapters. A suggested sequence of reading the book for a beginner would be: $1 \rightarrow 2 \rightarrow 3 \rightarrow 8 \rightarrow 11$, while for a more advanced reader the book is expected to be studied in entirety. We had tried our best to reduce the mistakes in the book, however we would be grateful if you report us via emails for any pending issues.

Happy Reading!

Kharagpur, India
August 2017

Sikhar Patranabis
Debdeep Mukhopadhyay

Acknowledgements

The authors would like to thank the following colleagues and fellow researchers for their graciously kind contributions, that have imparted immense value to the technical content of the book:

- Ms. Sarani Bhattacharya, Department of Computer Science and Engineering, IIT Kharagpur
- Mr. Sayandeep Saha, Department of Computer Science and Engineering, IIT Kharagpur
- Mr. Abhishek Chakraborty, Department of Computer Science and Engineering, IIT Kharagpur
- Dr. Jakub Breier, Temasek Laboratories, Nanyang Technological University, Singapore
- Dr. Shivam Bhasin, Temasek Laboratories, Nanyang Technological University, Singapore
- Dr. Dirmanto Jap, Temasek Laboratories, Nanyang Technological University, Singapore
- Dr. Wei He, Shield Lab, Central Research Institute, Huawei International Pte. Ltd., Singapore
- Dr. Chien-Ning Chen, Independent Researcher (Formerly with Division of Mathematical Sciences, School of Physical and Mathematical Sciences, NTU Singapore)

Debdeep would like to thank his parents for their constant blessings. He also expresses his gratitude to Prof. P. P. Chakrabarti for his constant guidance, encouragement, and wonderful technical ideas in spite of his busy schedule. He would also like to express his thanks to Prof. Anupam Chattopadhyay for encouraging him to write the book during his stay at NTU Singapore. He expresses his sincere thanks to all the contributory authors and collaborators, and, in particular, his student Sikhar Patranabis, for making the book see the light of the day. He would, in particular, like to mention the support of his wife for tolerating him and to his daughter Debanti for being the wind beneath his wings to fly high. Also, last but

not the least, he would like to thank his research students for having faith in him and his ideas.

Sikhar would like to thank his supervisor Dr. Debdeep Mukhopadhyay for his constant encouragement, motivation, and guidance. He also thanks his colleagues at the Secured Embedded Architecture Lab, Department of CSE, IIT Kharagpur for their inputs and assistance. He expresses his gratitude to his parents and uncle for their blessings and unwavering support. He would like to thank his maternal aunt and her husband, along with his cousin Ahanaa, for their support and encouragement. Finally, he would like to mention the role of his girlfriend Ria in being a constant source of support through the many ups and downs over the years.

Contents