Information Security and Cryptography

For further volumes:
http://www.springer.com/series/4752

Marc Joye · Michael Tunstall
Editors

Fault Analysis in Cryptography

Springer

Editors
Marc Joye
Technicolor
1 avenue de Belle Fontaine
Cesson-Sévigné Cedex
35576
France

Michael Tunstall
Department of Computer Science
University of Bristol
Woodland Road
Bristol
BS8 1UB
UK

ISSN 1619-7100
ISBN 978-3-642-29655-0 ISBN 978-3-642-29656-7 (eBook)
DOI 10.1007/978-3-642-29656-7
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2012939112

ACM Computing Classification: E.3, B.1

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)


Juliette Joye

Foreword

Fault attacks is an active area of research in cryptography, currently explored in hundreds of research papers and dedicated conferences. This book is the first comprehensive treatment of the subject covering both the theory and practice of these attacks as well as defense techniques.

Fault attacks exploit the fact that computers sometimes make mistakes. These mistakes can result from a programming error, as in the case of the infamous Intel floating-point bug. Or they can result from direct interference by an attacker, say by running the computer in a hostile environment. This book explores what happens to cryptographic algorithms when the computer implementing the algorithm makes a calculation error. Very often these errors, called faults, can have disastrous consequences, rendering the system completely insecure. As an extreme example, a single mistake during the calculation of an RSA digital signature can completely expose the signer's secret key to anyone who obtains the faulty signature. Over the years it has been shown that a wide range of cryptographic algorithms succumb to fault attacks. This book does a beautiful job of presenting powerful fault attacks against a wide range of systems.

Preventing fault attacks without sacrificing performance is nontrivial. Over the years a number of innovative ideas have been proposed for efficiently verifying cryptographic computations. Many defense strategies are described in the book, some of which are already deployed in real-world cryptographic libraries. Nevertheless, many implementations remain vulnerable. I was thrilled to see the material covered in the book and hope that it will make fault defense the standard practice in the minds of developers.

Dan Boneh
Stanford University

Preface

One of the first examples of fault injection in microprocessors was unintentional. May and Woods noticed that radioactive particles produced by elements present in the packaging materials used to protect microprocessors were energetic enough to cause faults [277]. Specifically, it was observed that α particles were released by uranium-235, uranium-238, and thorium-230 residues present in the packaging, decaying to lead-206. These particles were able to create a large enough charge that bits in sensitive areas of a chip could be made to flip. These elements were only present in two or three parts per million, but this concentration was sufficient to change the behavior of a microprocessor.

Further research into the physical effects that could affect the behavior of microprocessors included studying and simulating the effects of cosmic rays on semiconductors [435]. While the effect of cosmic rays are very weak at ground level because of the Earth's atmosphere, their effect becomes more pronounced in the upper atmosphere and outer space. This is important as faults in airborne electronic systems have potentially catastrophic consequences. This provoked research by organizations such as NASA and Boeing to "harden" electronic devices so that they are able to operate in harsh environments.

Since then other physical means of inducing errors have been discovered but all of these have had somewhat similar effect. In 1992, for example, Habing determined that a laser beam could be used to imitate the effect of charge particles on microprocessors [173]. The different faults that can be produced have been characterized to enable the design of suitable protection mechanisms.

The first academic publication that discussed using such a fault to intentionally break a cryptographic algorithm was described by Boneh, DeMillo, and Lipton in 1997 [56]. It was observed, among other things, that an implementation of RSA that uses the Chinese Remainder Theorem to compute a modular exponentiation is very sensitive to fault attacks (see Sect. 8.2). A similar publication followed this that described a fault to intentionally break a secret key cryptographic algorithm [49]. More specifically, this attack applied techniques from differential cryptanalysis that would allow an attacker to exploit a fault to break an implementation of DES (see Sect. 3.3).

Aumüller, Bier, Fischer, Hofreiter, and Seifert published the first academic paper detailing an implementation of one of these attacks [18]. They describe an implementation of the attack by Boneh et al. breaking an implementation of RSA computed using the Chinese Remainder Theorem.

Since then numerous attacks and countermeasures have been proposed and implemented. This book presents a summary of the state of the art in the theoretical and practical aspects of fault analysis and countermeasures. *Happy reading*!

Rennes (France), Bristol (UK), April 2011

Marc Joye
Michael Tunstall

Contents

Part I Introductory Material

1 **Side-Channel Analysis and Its Relevance to Fault Attacks** 3
Elisabeth Oswald and François-Xavier Standaert

Part II Fault Analysis in Secret Key Cryptography

2 **Attacking Block Ciphers** 19
Christophe Clavier

3 **Differential Fault Analysis of DES** 37
Matthieu Rivain

4 **Differential Fault Analysis of the Advanced Encryption Standard** 55
Christophe Giraud

5 **Countermeasures for Symmetric Key Ciphers** 73
Jörn-Marc Schmidt and Marcel Medwed

6 **On Countermeasures Against Fault Attacks on the Advanced Encryption Standard** 89
Kaouthar Bousselam, Giorgio Di Natale, Marie-Lise Flottes and Bruno Rouzeyre

Part III Fault Analysis in Public Key Cryptography

7 A Survey of Differential Fault Analysis Against Classical RSA Implementations 111
Alexandre Berzati, Cécile Canovas-Dumas and Louis Goubin

8 Fault Attacks Against RSA-CRT Implementation 125
Chong Hee Kim and Jean-Jacques Quisquater

9 Fault Attacks on Elliptic Curve Cryptosystems 137
Abdulaziz Alkhoraidly, Agustín Domínguez-Oviedo and M. Anwar Hasan

10 On Countermeasures Against Fault Attacks on Elliptic Curve Cryptography Using Fault Detection 157
Arash Hariri and Arash Reyhani-Masoleh

11 Design of Cryptographic Devices Resilient to Fault Injection Attacks Using Nonlinear Robust Codes 171
Kahraman D. Akdemir, Zhen Wang, Mark Karpovsky and Berk Sunar

12 Lattice-Based Fault Attacks on Signatures 201
Phong Q. Nguyen and Mehdi Tibouchi

13 Fault Attacks on Pairing-Based Cryptography 221
Nadia El Mrabet, Dan Page and Frederik Vercauteren

Part IV Miscellaneous

14 Fault Attacks on Stream Ciphers 239
Alessandro Barenghi and Elena Trichina

15 Interaction Between Fault Attack Countermeasures and the Resistance Against Power Analysis Attacks 257
Francesco Regazzoni, Luca Breveglieri, Paolo Ienne and Israel Koren

Part V Implementing Fault Attacks

16 Injection Technologies for Fault Attacks on Microprocessors 275
Alessandro Barenghi, Guido M. Bertoni, Luca Breveglieri, Mauro Pelliccioli and Gerardo Pelosi

17 Global Faults on Cryptographic Circuits 295
Sylvain Guilley and Jean-Luc Danger

18 Fault Injection and Key Retrieval Experiments on an Evaluation Board 313
Junko Takahashi, Toshinori Fukunaga, Shigeto Gomisawa, Yang Li, Kazuo Sakiyama and Kazuo Ohta

References 333

Contributors

Kahraman D. Akdemir Worcester Polytechnic Institute, USA

Abdulaziz Alkhoraidly University of Waterloo, Waterloo, Canada

Alessandro Barenghi Politecnico di Milano, Italy

Alexandre Berzati CEA Leti, France

Guido M. Bertoni STMicroelectronics, Italy

Kaouthar Bousselam Université de Montpellier II, France

Luca Breveglieri Politecnico di Milano, Milan, Italy

Cécile Canovas-Dumas CEA Leti, France

Christophe Clavier XLIM & Université de Limoges, France

Jean-Luc Danger Telecom ParisTech, France

Giorgio Di Natale LIRMM / CNRS, France

Agustín Domínguez-Oviedo Tecnológico de Monterrey, Mexico

Nadia El Mrabet Université de Caen, France

Marie-Lise Flottes LIRMM / CNRS, France

Toshinori Fukunaga NTT Information Sharing Platform Laboratories, Japan

Christophe Giraud Oberthur Technologies, France

Shigeto Gomisawa The University of Electro-Communications, Japan

Louis Goubin Université de Versailles Saint-Quentin-en-Yvelines, France

Sylvain Guilley Telecom ParisTech, France

Arash Hariri The University of Western Ontario, Canada

M. Anwar Hasan University of Waterloo, Waterloo, Canada

Paolo Ienne École Polytechnique Fédérale de Lausanne, Switzerland

Mark Karpovsky Boston University, USA

Chong Hee Kim Université Catholique de Louvain, Belgium

Israel Koren University of Massachusetts, USA

Yang Li The University of Electro-Communications, Japan

Marcel Medwed Université Catholique de Louvain, Belgium; Graz University of Technology, Austria

Phong Q. Nguyen École Normale Supérieure, France

Kazuo Ohta The University of Electro-Communications, Japan

Elisabeth Oswald University of Bristol, UK

Dan Page University of Bristol, UK

Mauro Pelliccioli Politecnico di Milano, Italy

Gerardo Pelosi Politecnico di Milano, Italy

Jean-Jacques Quisquater Université Catholique de Louvain, Belgium

Francesco Regazzoni Université Catholique de Louvain, Belgium; University of Lugano, Switzerland

Arash Reyhani-Masoleh The University of Western Ontario, Canada

Matthieu Rivain CryptoExperts, France

Bruno Rouzeyre Université de Montpellier II, France

Kazuo Sakiyama The University of Electro-Communications, Japan

Jörn-Marc Schmidt Graz University of Technology, Austria

François-Xavier Standaert Université Catholique de Louvain, Belgium

Berk Sunar Worcester Polytechnic Institute, USA

Junko Takahashi NTT Information Sharing Platform Laboratories, The University of Electro-Communications, Japan

Mehdi Tibouchi École Normale Supérieure, France

Elena Trichina STMicroelectronics, Italy

Frederik Vercauteren Katholieke Universiteit Leuven, Belgium

Zhen Wang Boston University, USA