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

http://www.springer.com/978-3-642-29655-0

Fault Analysis in Cryptography
Joye, M.; Tunstall, M. (Eds.)
2012, XVI, 356 p., Hardcover
ISBN: 978-3-642-29655-0