Springer

密码故障分析与防护

Fault Analysis in Cryptography

[法] Marc Joye
[英] Michael Tunstall 编著
赵新杰 郭世泽 张 帆 谷大武 译

科学出版社

密码故障分析与防护

Fault Analysis in Cryptography

〔法〕Marc Joye
〔英〕Michael Tunstall 编著

赵新杰　郭世泽　张 帆　谷大武　译

科 学 出 版 社

北 京

图字：01-2015-0275 号

内 容 简 介

密码设备运行环境在受到外界干扰时，密码运算会被注入故障从而产生错误，利用这些错误信息进行的密码分析称为密码故障分析。当前，故障分析攻击已对各类密码模块的安全性构成了严峻的威胁。本书是国际上第一本关于密码故障分析与防护的综合性编著，系统地阐述了针对不同密码算法实现的故障分析原理、技术方法以及防护对策。

全书共 5 个部分，由 18 章组成。第 1 章为第一部分，介绍了密码旁路分析和故障分析的关系。第 2~6 章为第二部分，阐述了分组密码故障分析与防护技术。第 7~13 章为第三部分，阐述了公钥密码故障分析与防护技术。第 14~15 章为第四部分，阐述了序列密码故障分析与防护技术，以及攻击防护措施对密码实现抗功耗旁路攻击的影响。第 16~18 章为第五部分，给出了故障注入技术及物理实验细节。

本书可作为网络空间安全、密码学、计算机科学、微电子学等专业高年级本科生和研究生相关课程的教材，也可供相关领域的教学、科研和工程技术人员阅读参考。

图书在版编目（CIP）数据

密码故障分析与防护 Fault Analysis in Cryptography /（法）马克裘依（Marc, J.），（英）腾斯托尔（Tunstall, M.）编著；赵新杰等译.—北京：科学出版社, 2015
ISBN 978-7-03-045022-7

Ⅰ.①密… Ⅱ.①马…②腾…③赵… Ⅲ.①密码算法 Ⅳ.①TN918.1

中国版本图书馆 CIP 数据核字 (2015) 第 131015 号

责任编辑：陈 静 纪四稳 / 责任校对：郭瑞芝
责任印制：徐晓晨 / 封面设计：迷底书装

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

北京中石油彩色印刷有限责任公司 印刷
科学出版社发行 各地新华书店经销
*
2015 年 11 月第 一 版 开本：720×1 000 B5
2015 年 11 月第一次印刷 印张：21 插页：2
字数：401 000

定价：88.00 元

（如有印装质量问题，我社负责调换）

贡献者

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 Universit é 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 Ècole Normale Supérieure, France

Elena Trichina STMicroelectronics, Italy

Frederik Vercauteren Katholieke Universiteit Leuven, Belgium

Zhen Wang Boston University, USA

中 文 版 序

“没有网络安全就没有国家安全”。在全新的网络化、智能化、信息化时代，国家安全的现实需求为网络安全提出了更高要求。作为网络安全核心技术之一的密码技术也相应地出现了新的发展趋势。

一方面，随着密码算法设计技术和可证明安全理论的发展，密码算法的设计技术越来越完善，使得传统差分分析、线性分析等方法难以在有限复杂度内奏效。以至于美国密码学家 Kahn 悲观地指出“很多密码系统如今都不能用已知的密码分析方法来破解，从某种意义上来说，密码分析已经死了。”但另一方面，密码算法的应用环境从军事保密环境逐渐走向计算机网络、通信终端、金融支付等开放网络环境，攻击者所能进行的动作和获取的资源远远超过教科书中的假设，为密码分析又带来了新的机会。1996 年，美国密码学家 Kocher 等发现：现代密码系统在设计上的理论安全性并不等同于实现中的物理安全性，密码算法在运行过程中会无意泄露出执行时间差异信息，即所谓的旁路信息，通过观测这些旁路信息，攻击者可以采用“分而治之”的方式逐片段地恢复密钥，这类密码分析被称为计时旁路分析。在此基础上，研究者又发现了功耗、电磁辐射、声音等旁路泄露，并提出了相应的密码旁路分析方法。

根据唯物辩证法中联系的普遍性和多样性原理，攻击者除了能够观测密码运行过程中无意产生的旁路泄露，也应该可以主动地干扰和影响密码运行过程，利用得到的其他类旁路信息进行密码分析。1997 年，美国斯坦福大学教授 Boneh 等发现：智能卡上的 RSA 签名实现在受到外界环境干扰 (如时钟、电压、辐射等突变) 时，密码电路会被注入故障，从而产生错误的签名输出。攻击者通过对一次错误签名分析即可攻破 RSA 签名算法，这种密码分析被称为故障分析或故障攻击。此后，故障分析陆续被扩展至几乎所有的密码算法，如 ECC、DSA 等公钥密码算法，DES、AES 等分组密码算法，RC4、Trivium 等序列密码算法。

由于现代密码设备大都基于电子技术实现，接口相对比较简单，工作过程中较易受到外界条件的干扰，故障注入的可行性较高，对其进行防护极为困难。同时，和计时、功耗、电磁等旁路分析方法相比，故障分析的数据复杂度相对较低。以 DES、AES、RSA 等密码攻击为例，1 次故障注入分析即可恢复完整密钥。鉴于故障注入的现实可行性和分析方法的高效性，故障分析目前已经成为密码实现物理安全性的最大威胁之一。故障分析与防护研究逐渐成为密码学研究中的一个重要分支，得到了国际学术界与产业界的广泛关注。例如，在美国国家标准与技术研究所发布的密码模块安全标准第三版 FIPS 140-3 中，首次将故障分析明确提案

至 4.6 节物理安全部分，要求密码设备在设计、生产、使用过程中必须加强故障分析防护。

在承担多项旁路分析和故障分析相关的国家 973、国家自然科学基金项目的基础上，课题组之前出版了《密码旁路分析原理与方法》专著，对常见的分组密码、公钥密码、序列密码算法的旁路分析技术进行了介绍，并对故障分析技术有了初步的涉及。为了更加全面地介绍密码故障分析与防护技术，我们选取了 Springer 出版的*Fault Analysis in Cryptography* 一书，并组织课题组成员进行了翻译，希望对国内密码学的研究与密码技术的应用起到一定的推动作用。

故障分析是什么？实施故障分析需要什么样的设备与技术条件？这种分析对密码算法在密码设备中的实际安全性将会造成什么样的影响？如何设计实现可靠、高效、低廉的防护对策来有效地防御此类分析？如何客观、合理地评估各种防护措施的有效性？故障分析防御对策抗功耗分析等其他类型旁路分析的能力如何？本书是国际上第一本系统介绍密码故障分析理论、实践以及防护措施的一本编著，由 Techniolor 集团的杰出科学家 Joye 和英国布里斯托大学密码学教授 Tunstall 等牵头编著，全书所有章节由国际上 47 位从事旁路分析与故障分析研究的知名密码学家联合撰写，将会对上述问题进行详细地解答。

全书共 5 个部分，由 18 个章节组成。第 1 章为第一部分，介绍了密码旁路分析和故障分析的关系，读者可以了解简单功耗分析、差分功耗分析如何被用于故障注入的触发。第 2~6 章为第二部分，阐述了分组密码的故障分析与防护技术，读者可以了解 DES、AES 等分组密码故障分析与防护技术进展，尤其是差分故障分析、碰撞故障分析、无效故障分析、安全错误分析、轮次修改故障分析等方法，以及基于模块冗余、编码理论、协议层级的故障分析防护对策。第 7~13 章为第三部分，阐述了公钥密码故障分析与防护技术，读者可以了解经典的 RSA、ECC 等公钥密码故障分析方法，基于非线性鲁棒编码的抗故障分析电路设计，故障分析与格基规约的结合应用和针对配对密码学的分析技术。第 14~15 章为第四部分，阐述了序列密码故障分析与防护技术和已有故障分析防护措施的安全性，读者可以了解 RC4、Trivium、HC-128 等序列密码的故障分析方法与典型防御对策，以及不同策略的故障分析防护措施对密码实现抗功耗旁路分析的影响。第 16~18 章为第五部分，给出了故障注入技术及物理实验细节，读者可以了解不同成本的故障注入技术、常用处理器的亏电故障注入技术、FPGA/ASIC 密码电路的全局故障注入技术以及针对旁路攻击评估板的故障攻击物理实验细节。

本书可作为网络空间安全、密码学、计算机科学、微电子学等专业高年级本科生和研究生相关课程的教材，也可供相关领域的教学、科研和工程技术人员阅读参考。在本书的翻译过程中，项目组的多位老师、研究生都付出了辛勤的劳动，他们是上海交通大学的郭筝、顾海华博士，中国人民解放军军械工程学院的刘会英、周

平、冀可可、陈浩、张金中、吴克辉等研究生，浙江大学的沈继忠教授和耿亮、许聪源等研究生，美国康涅狄格大学的蔡兴宇等研究生。特别感谢军械工程学院王韬教授对全书翻译提出的很多指导和建设性意见！此外，考虑到本书涉及面较广，为了确保翻译准确、阅读流畅，我们还有幸得到了国内很多密码界同行的指导和帮助。北京理工大学的王安博士、国防科学技术大学的李瑞林博士对分组密码故障分析与防护方面的章节进行了校对；电子科技大学的李发根教授和张秀洁博士、中国科学院信息工程研究所的孙思维博士对公钥密码故障分析与防护方面的章节进行了校对；中国人民解放军信息工程大学的关杰教授对序列密码故障分析与防护方面的章节进行了校对；南京航空航天大学的李阳副教授、国民技术股份有限公司的张翌维博士和王宇建工程师对故障攻击物理实验相关的章节进行了校对，在此一并表示衷心的感谢！

本书的翻译工作得到了国家 973 计划 (项目编号：2013CB338004)、国家自然科学基金项目 (项目编号：60772082、61073150、61173191、61272491、61202386、61309021、61472357、61571063)、浙江大学青年科研创新专项基金 (项目编号：2015QNA5005) 的资助，特此致谢！

“奇法当然显异工，寻机探秘境无穷，辛勤自有成功日，击节推杯唱大风。”随着密码应用环境的变化和密码分析技术的发展，密码学将与数学、物理、计算机、微电子、通信、网络等学科深度融合，我们现在所看到的密码故障分析与防护技术只是冰山一角，尚有大量认识不清、理论不足、验证不够的研究领域，亟待我们抱着科学的态度去研究、探索、发现。正如我们团队的座右铭所言：前面的高山是如此巍峨美丽，让我们一起去攀登吧！

限于水平，书中难免有错误和不足之处，恳请读者批评指正！

译　者

2015 年 10 月于北京

序

故障攻击是密码学中的一个热门领域，当前已经有数以百计相关的研究论文和专业会议论文。本书是第一本从理论和实际、攻击和防御等多个角度来系统阐述这一主题的著作。

故障攻击主要利用计算机运行时有时会出现错误的客观事实。这些错误可能来自编程错误，如 20 世纪 90 年代广为人知的 Intel 浮点除错误，或者来自攻击者的主动干扰，如将计算机运行在一个恶意的环境中。本书主要挖掘计算机实现密码算法时出现的运算错误。一般来说，计算机一旦发生这些错误，又称故障，会产生难以估量的毁灭性结果，使得整个系统不再安全。举一个极端的例子，RSA 签名过程中的一次错误就有可能使获得错误签名的任何人获取签名者的私钥。近年来的研究表明，大多数的密码算法都不能抵抗故障攻击。本书给出了针对大量密码系统进行故障攻击的出色的研究工作。

在防御故障攻击的同时不牺牲效率也不是不可能的。近年来，大量的创新性想法被提出并用于快速检验密码运算的正确性。本书给出了很多故障攻击的防御措施，其中很多已经被部署应用到现实的密码库中。不可否认的是，很多密码实现仍然是不安全的。我十分激动地看到本书给出了很多故障攻击的防御实现，也希望密码开发者能够通过本书认识到故障攻击防御在实践中是多么的重要。

Dan Boneh
斯坦福大学

前　言

针对微控制器的首例故障注入纯属偶然。May 和 Woods 注意到用来保护微处理器的封装材料中的放射性微粒容易产生故障[277]。特别是封装中的微粒物会释放铀 -235、铀 -238、钍 -230，并衰减为铅 -206。这些微粒物会产生足够大的电流使得芯片上敏感区域的比特产生翻转。虽然这些元素只占百万分之二或三，但足以改变微处理器的行为。

后续关于影响微处理器的物理特征研究包括学习和仿真宇宙射线对半导体的影响 [435]。由于地球大气层的影响，地面上的宇宙射线产生的影响十分微弱，而在大气层顶部或者外太空，宇宙射线产生的影响则比较显著。鉴于故障对航空电子系统的影响则是灾难性的，美国国家航空与航天局 (National Aeronautics and Space Administration，NASA) 和波音公司 (Boeing) 组织发起了如何在复杂环境下对电子设备进行抗干扰的研究。

从那时起，通过其他物理方式来注入故障被大量地发现，但是它们都具有一定程度上的相似性。1992 年，Habing 发现一个激光束可以伪造微处理器上微粒物的充电效应[173]，产生的不同的错误可以被刻画出来，进而指导相应的防御机制设计。

在学术界，Boneh、DeMillo 和 Lipton 在 1997 年[56] 给出了首例使用故障方式来破解密码算法的攻击。他们指出，使用中国剩余定理的 RSA 实现在计算模幂运算时很容易遭受故障攻击 (具体见本书 8.2 节)。之后，文献 [49] 给出了如何基于故障对私钥密码算法进行攻击。具体来说，这种由差分分析演变而来的差分故障攻击使得攻击者可以通过挖掘故障来攻破 DES 分组密码的一种实现 (具体见本书 3.3 节)。

Aumüller、Bier、Fischer、Hofreiter 和 Seifert 给出了详细实现这些攻击的首例学术论文[18]，他们实现了 Boneh 等针对使用中国剩余定理算法实现的 RSA 故障攻击。

之后，大量的故障攻击和防护措施被提出或实现。本书从理论与实践两个角度给出了密码故障分析和防御领域的研究现状，祝您阅读愉快!

Marc Joye, Michael Tunstall

2011 年 4 月于雷恩 (法国)，布里斯托 (英国)

目　　录

绪　　论

私钥密码体制故障分析

公钥密码体制故障分析

混合部分

故障攻击实现