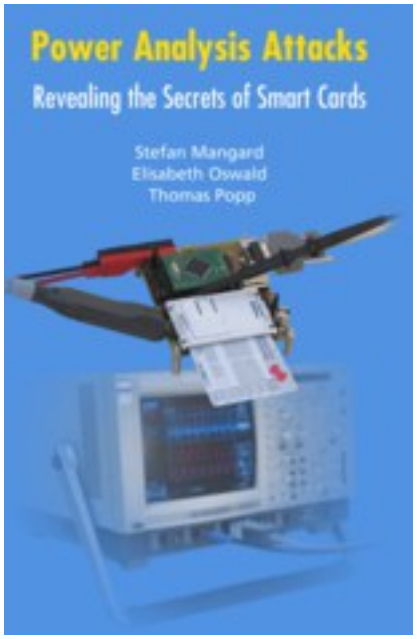
Power Analysis Attacks



Power Analysis Attacks_下载链接1_

著者:Mangard, Stefan/ Oswald, Elisabeth/ Popp, Thomas

出版者:Springer Verlag

出版时间:2007-3

装帧:HRD

isbn:9780387308579

Power analysis attacks allow the extraction of secret information from smart cards. Smart cards are used in many applications including banking, mobile communications, pay TV, and electronic signatures. In all these applications, the security of the smart cards is of crucial importance. Power Analysis Attacks: Revealing the Secrets of Smart Cards is the first comprehensive treatment of power analysis attacks and countermeasures. Based on the principle that the only way to defend against power analysis attacks is to understand them, this book explains how power analysis attacks work. Using many examples, it discusses simple and differential power analysis as well as advanced techniques like template attacks. Furthermore, the authors provide an extensive discussion of countermeasures like shuffling, masking, and DPA-resistant logic styles. By analyzing the pros and cons of the different

countermeasures, this volume allows practitioners to decide how to protect smart cards.

作者介绍:

目录:

Power Analysis Attacks_下载链接1_

标签

信道攻击

外文书籍

评论

Power Analysis Attacks_下载链接1_

书评

Power Analysis Attacks_下载链接1_