



Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security)

By Stefan Mangard, Elisabeth Oswald, Thomas Popp

[Download now](#)

[Read Online](#) 

Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security) By Stefan Mangard, Elisabeth Oswald, Thomas Popp

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.

 [Download Power Analysis Attacks: Revealing the Secrets of S ...pdf](#)

 [Read Online Power Analysis Attacks: Revealing the Secrets of ...pdf](#)

Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security)

By Stefan Mangard, Elisabeth Oswald, Thomas Popp

Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security) By Stefan Mangard, Elisabeth Oswald, Thomas Popp

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.

Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security) By Stefan Mangard, Elisabeth Oswald, Thomas Popp **Bibliography**

- Sales Rank: #2053903 in Books
- Published on: 2007-03-12
- Original language: English
- Number of items: 1
- Dimensions: 9.21" h x .81" w x 6.14" l, 1.59 pounds
- Binding: Hardcover
- 338 pages

 [Download Power Analysis Attacks: Revealing the Secrets of S ...pdf](#)

 [Read Online Power Analysis Attacks: Revealing the Secrets of ...pdf](#)

Download and Read Free Online Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security) By Stefan Mangard, Elisabeth Oswald, Thomas Popp

Editorial Review

From the Back Cover

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, this volume provides an extensive discussion of countermeasures like shuffling, masking, and DPA-resistant logic styles.

By analyzing the pros and cons of the different countermeasures, **Power Analysis Attacks: Revealing the Secrets of Smart Cards** allows practitioners to decide how to protect smart cards. This book also provides valuable information for graduate and advanced undergraduate students, and researchers working in information security.

Users Review

From reader reviews:

Aaron Tyler:

Have you spare time for just a day? What do you do when you have more or little spare time? Yeah, you can choose the suitable activity to get spend your time. Any person spent their own spare time to take a go walking, shopping, or went to typically the Mall. How about open or even read a book eligible Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security)? Maybe it is to be best activity for you. You realize beside you can spend your time using your favorite's book, you can more intelligent than before. Do you agree with its opinion or you have various other opinion?

Keith Smith:

This book untitled Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security) to be one of several books that best seller in this year, that is because when you read this reserve you can get a lot of benefit into it. You will easily to buy that book in the book retailer or you can order it via online. The publisher on this book sells the e-book too. It makes you more readily to read this book, because you can read this book in your Smartphone. So there is no reason for you to past this reserve from your list.

Betty Borgen:

A lot of people always spent their particular free time to vacation or perhaps go to the outside with them family or their friend. Did you know? Many a lot of people spent they free time just watching TV, or even playing video games all day long. If you want to try to find a new activity that is look different you can read any book. It is really fun for yourself. If you enjoy the book which you read you can spent the whole day to reading a e-book. The book Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security) it is very good to read. There are a lot of those who recommended this book. These people were enjoying reading this book. Should you did not have enough space to deliver this book you can buy often the e-book. You can m0ore simply to read this book from the smart phone. The price is not very costly but this book features high quality.

Maurice Lamothe:

People live in this new day time of lifestyle always try to and must have the extra time or they will get large amount of stress from both daily life and work. So , once we ask do people have free time, we will say absolutely without a doubt. People is human not just a robot. Then we ask again, what kind of activity do you possess when the spare time coming to an individual of course your answer can unlimited right. Then ever try this one, reading textbooks. It can be your alternative with spending your spare time, the particular book you have read is usually Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security).

Download and Read Online Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security) By Stefan Mangard, Elisabeth Oswald, Thomas Popp #Z25DP91863S

Read Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security) By Stefan Mangard, Elisabeth Oswald, Thomas Popp for online ebook

Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security) By Stefan Mangard, Elisabeth Oswald, Thomas Popp Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security) By Stefan Mangard, Elisabeth Oswald, Thomas Popp books to read online.

Online Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security) By Stefan Mangard, Elisabeth Oswald, Thomas Popp ebook PDF download

Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security) By Stefan Mangard, Elisabeth Oswald, Thomas Popp Doc

Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security) By Stefan Mangard, Elisabeth Oswald, Thomas Popp Mobipocket

Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security) By Stefan Mangard, Elisabeth Oswald, Thomas Popp EPub

Z25DP91863S: Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security) By Stefan Mangard, Elisabeth Oswald, Thomas Popp