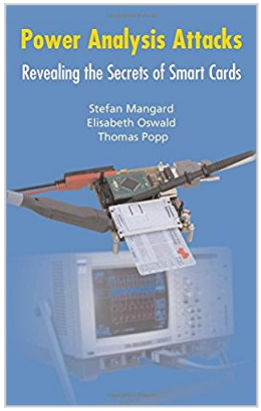

Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security)

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

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

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:

Kevin Kennard:

As people who live in the actual modest era should be upgrade about what going on or facts even knowledge to make these people keep up with the era which can be always change and move ahead. Some of you maybe will probably update themselves by reading books. It is a good choice to suit your needs but the problems coming to an individual is you don't know what kind you should start with. This Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security) is our recommendation to cause you to keep up with the world. Why, because book serves what you want and need in this era.

Glenn Bail:

Playing with family in a park, coming to see the marine world or hanging out with close friends is thing that usually you could have done when you have spare time, subsequently why you don't try factor that really opposite from that. A single activity that make you not experience tired but still relaxing, trilling like on roller coaster you are ride on and with addition of information. Even you love Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security), you could enjoy both. It is good combination right, you still need to miss it? What kind of hang-out type is it? Oh can occur its mind hangout

fellas. What? Still don't buy it, oh come on its named reading friends.

Michael Sheridan:

Does one one of the book lovers? If so, do you ever feeling doubt if you find yourself in the book store? Try and pick one book that you find out the inside because don't determine book by its handle may doesn't work at this point is difficult job because you are scared that the inside maybe not since fantastic as in the outside appear likes. Maybe you answer is usually Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security) why because the excellent cover that make you consider in regards to the content will not disappoint a person. The inside or content is definitely fantastic as the outside as well as cover. Your reading 6th sense will directly assist you to pick up this book.

Fred Peterson:

Are you kind of stressful person, only have 10 or maybe 15 minute in your day time to upgrading your mind ability or thinking skill also analytical thinking? Then you are experiencing problem with the book in comparison with can satisfy your short time to read it because all this time you only find e-book that need more time to be go through. Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security) can be your answer since it can be read by anyone who have those short free time problems.

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

MX6HBFWVU4Z: Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security) By Stefan Mangard, Elisabeth Oswald, Thomas Popp