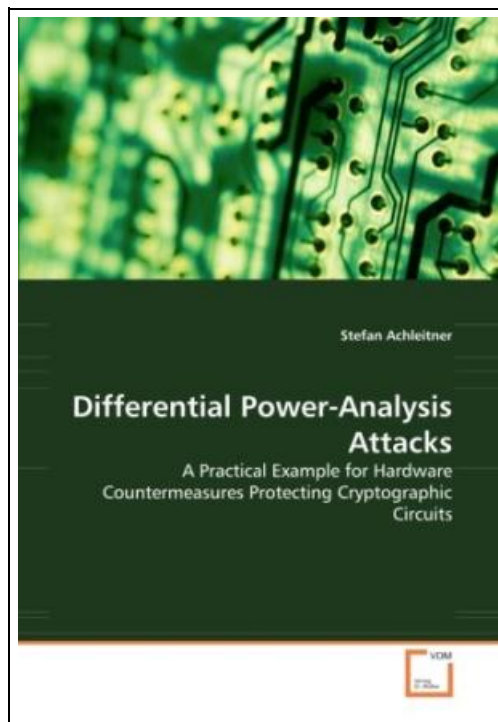


## Differential Power-Analysis Attacks



Filesize: 6.27 MB

### **Reviews**

*This ebook can be worthy of a read, and much better than other. I have read and i am certain that i am going to planning to go through again once again in the future. You may like just how the writer compose this book.*  
*(Mr. Grant Stanton PhD)*

## DIFFERENTIAL POWER-ANALYSIS ATTACKS



To save **Differential Power-Analysis Attacks** eBook, remember to follow the button under and download the document or have accessibility to additional information that are highly relevant to DIFFERENTIAL POWER-ANALYSIS ATTACKS ebook.

Condition: New. Publisher/Verlag: VDM Verlag Dr. Müller | A Practical Example for Hardware Countermeasures Protecting Cryptographic Circuits | Implementations of theoretically secure cryptographic algorithms can be broken by side-channel attacks. In particular, block ciphers have turned out to be very susceptible to differential power-analysis (DPA) attacks. Various methods to prevent these attacks have been proposed so far. This book is about countermeasures against DPA attacks, which can be easily implemented in a standard CMOS design flow. In particular, the work focuses on the insertion of dummy operations, on the randomization of operands and on the generation of noise. The effectiveness and the costs of these countermeasures are analyzed. In addition, an ASIC design implementing these countermeasures is presented. The design is a strong authentication module using AES equipped with the countermeasures. First measurement results of this design based on an FPGA prototype are also part of this book. Not only researchers in the area of cryptography and security are addressed by this work but also hardware security designers. | Format: Paperback | Language/Sprache: english | 125 gr | 220x150x4 mm | 84 pp.



[Read Differential Power-Analysis Attacks Online](#)

[Download PDF Differential Power-Analysis Attacks](#)

## You May Also Like

---

**[PDF] Would It Kill You to Stop Doing That?**

Follow the link below to download "Would It Kill You to Stop Doing That?" PDF document.

[Save](#) [eBook](#)

»

---

**[PDF] Violet Rose and the Surprise Party**

Follow the link below to download "Violet Rose and the Surprise Party" PDF document.

[Save](#) [eBook](#)

»

---

**[PDF] Chris P. Bacon: My Life So Far.**

Follow the link below to download "Chris P. Bacon: My Life So Far." PDF document.

[Save](#) [eBook](#)

»

---

**[PDF] Public Opinion + Conducting Empirical Analysis**

Follow the link below to download "Public Opinion + Conducting Empirical Analysis" PDF document.

[Save](#) [eBook](#)

»

---

**[PDF] How to Make a Free Website for Kids**

Follow the link below to download "How to Make a Free Website for Kids" PDF document.

[Save](#) [eBook](#)

»

---

**[PDF] The Trouble with Trucks: First Reading Book for 3 to 5 Year Olds**

Follow the link below to download "The Trouble with Trucks: First Reading Book for 3 to 5 Year Olds" PDF document.

[Save](#) [eBook](#)

»