Why Cryptography Should Not Rely on Physical Attack Complexity (T-Labs Series in Telecommunication Services)

Juliane Krämer

Why Cryptography Should Not Rely on Physical Attack Complexity (T-Labs Series in Telecommunication Services)

Juliane Krämer

Why Cryptography Should Not Rely on Physical Attack Complexity (T-Labs Series in Telecommunication Services) Juliane Krämer

This book presents two practical physical attacks. It shows how attackers can reveal the secret key of symmetric as well as asymmetric cryptographic algorithms based on these attacks, and presents countermeasures on the software and the hardware level that can help to prevent them in the future. Though their theory has been known for several years now, since neither attack has yet been successfully implemented in practice, they have generally not been considered a serious threat. In short, their physical attack complexity has been overestimated and the implied security threat has been underestimated.

First, the book introduces the photonic side channel, which offers not only temporal resolution, but also the highest possible spatial resolution. Due to the high cost of its initial implementation, it has not been taken seriously. The work shows both simple and differential photonic side channel analyses. Then, it presents a fault attack against pairing-based cryptography. Due to the need for at least two independent precise faults in a single pairing computation, it has not been taken seriously either.

Based on these two attacks, the book demonstrates that the assessment of physical attack complexity is error-prone, and as such cryptography should not rely on it. Cryptographic technologies have to be protected against all physical attacks, whether they have already been successfully implemented or not. The development of countermeasures does not require the successful execution of an attack but can already be carried out as soon as the principle of a side channel or a fault attack is sufficiently understood.

Download and Read Free Online Why Cryptography Should Not Rely on Physical Attack Complexity (T-Labs Series in Telecommunication Services) Juliane Krämer

---

From reader reviews:

Stanley Hanson:

In other case, little folks like to read book Why Cryptography Should Not Rely on Physical Attack Complexity (T-Labs Series in Telecommunication Services). You can choose the best book if you like reading a book. Provided that we know about how is important any book Why Cryptography Should Not Rely on Physical Attack Complexity (T-Labs Series in Telecommunication Services). You can add information and of course you can around the world by the book. Absolutely right, due to the fact from book you can recognize everything! From your country until eventually foreign or abroad you will end up known. About simple thing until wonderful thing you could know that. In this era, we could open a book or searching by internet system. It is called e-book. You may use it when you feel bored to go to the library. Let's go through.

Richard Dutton:

Book is to be different for every grade. Book for children until finally adult are different content. As it is known to us that book is very important for people. The book Why Cryptography Should Not Rely on Physical Attack Complexity (T-Labs Series in Telecommunication Services) ended up being making you to know about other know-how and of course you can take more information. It is extremely advantages for you. The reserve Why Cryptography Should Not Rely on Physical Attack Complexity (T-Labs Series in Telecommunication Services) is not only giving you more new information but also to be your friend when you truly feel bored. You can spend your own spend time to read your e-book. Try to make relationship while using book Why Cryptography Should Not Rely on Physical Attack Complexity (T-Labs Series in Telecommunication Services). You never experience lose out for everything should you read some books.

Gladys Dearth:

Do you one of the book lovers? If so, do you ever feeling doubt if you are in the book store? Aim to pick one book that you never know the inside because don't evaluate book by its cover may doesn't work at this point is difficult job because you are afraid that the inside maybe not while fantastic as in the outside seem likes. Maybe you answer may be Why Cryptography Should Not Rely on Physical Attack Complexity (T-Labs Series in Telecommunication Services) why because the wonderful cover that make you consider in regards to the content will not disappoint an individual. The inside or content is fantastic as the outside or maybe cover. Your reading 6th sense will directly assist you to pick up this book.

Catherine Lyons:

As a student exactly feel bored in order to reading. If their teacher questioned them to go to the library or make summary for some book, they are complained. Just small students that has reading's internal or real their hobby. They just do what the instructor want, like asked to the library. They go to right now there but nothing reading really. Any students feel that reading through is not important, boring in addition to can't see

colorful photographs on there. Yeah, it is for being complicated. Book is very important to suit your needs. As we know that on this period of time, many ways to get whatever we wish. Likewise word says, many ways to reach Chinese's country. Therefore , this Why Cryptography Should Not Rely on Physical Attack Complexity (T-Labs Series in Telecommunication Services) can make you truly feel more interested to read.

Read Why Cryptography Should Not Rely on Physical Attack Complexity (T-Labs Series in Telecommunication Services) by Juliane Krämer for online ebook

Why Cryptography Should Not Rely on Physical Attack Complexity (T-Labs Series in Telecommunication Services) by Juliane Krämer 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 Why Cryptography Should Not Rely on Physical Attack Complexity (T-Labs Series in Telecommunication Services) by Juliane Krämer books to read online.

Online Why Cryptography Should Not Rely on Physical Attack Complexity (T-Labs Series in Telecommunication Services) by Juliane Krämer ebook PDF download

Why Cryptography Should Not Rely on Physical Attack Complexity (T-Labs Series in Telecommunication Services) by Juliane Krämer Doc

Why Cryptography Should Not Rely on Physical Attack Complexity (T-Labs Series in Telecommunication Services) by Juliane Krämer Mobipocket

Why Cryptography Should Not Rely on Physical Attack Complexity (T-Labs Series in Telecommunication Services) by Juliane Krämer EPub