1.

Record Nr.	UNINA9910746970003321
Autore	Zajic Alenka
Titolo	Understanding Analog Side Channels Using Cryptography Algorithms / / by Alenka Zaji, Milos Prvulovic
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2023
ISBN	3-031-38579-9
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (474 pages)
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Electronic circuits Data protection Telecommunication Cryptology Electronic Circuits and Systems Data and Information Security Communications Engineering, Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Preface -- I Introduction -- Ii What Is An Analog Side Channel? -- Iii Analog Side Channels -- Iv Unintentionally Modulated Side Channels -- V Relationship Between Modulated Side Channels And Program Activity -- Vi Parameters That Affect Analog Side Channels -- Vii Modeling Analog Side Channels as Communication Systems -- Viii Using Analog Side-Channels For Malware Detection -- Ix Using Analog Side Channels For Program Profiling -- X Using Analog Side Channels For Hardware Event Profiling -- Xi Using Analog Side Channels for Hardware/Software Attestation -- Xii Using Analog Side Channels For Hardware Identification -- Xiii Using Analog Side Channels To Attack Cryptographic Implementations -- Xiv Using Analog Side Channels For Hardware Trojan Detection.
Sommario/riassunto	This book offers the latest research results on analog side channels and their usage in cybersecurity. It demystifies analog side channels and

demonstrates new use cases for them. The first part of this book discusses how analog side channels are generated, the physics behind it, the modeling and measurements of analog side channels, and their analogies to wireless communication systems. The second part of this book introduces new applications that benefit from leveraging side channels. In addition to breaking cryptography algorithms, it demonstrates how analog side channels can be used for malware detection, program profiling, hardware profiling, hardware/software attestation, hardware identification, and hardware Trojan detection. Side channel is one of the methods for obtaining information about program execution. Traditionally, they are used in computer science to extract information about a key in cryptographic algorithms. What makes them different from other ways of extracting information about program execution is that side channels rely on how a system implements program execution, rather than what the program's algorithm specifies. Analog side channels are particularly powerful because they are not easy to suppress or detect that someone is collecting information from the system. Although they are very powerful tools, they are poorly understood. This book targets advanced level students in computer science and electrical engineering as a textbook. Researchers and professionals working with analog side channels, how to model them, measure them, improve signal to noise ratio, and invent new signal processing techniques can also use this book. Computer scientists and engineers who want to learn new applications of side channels to improve system security, new techniques for breaking cryptography keys, new techniques for attestation, and new techniques for hardware Trojan detection will also want to purchase this book.