1. Record Nr. UNINA9910299844403321

Autore	Rebeiro Chester
Titolo	Timing Channels in Cryptography : A Micro-Architectural Perspective / / by Chester Rebeiro, Debdeep Mukhopadhyay, Sarani Bhattacharya
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
ISBN	3-319-12370-X
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (162 p.)
Disciplina	005.74 620 621.382
Soggetti	Signal processing Image processing Speech processing systems Data structures (Computer science) Signal, Image and Speech Processing Data Structures and Information Theory
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	An Introduction to Timing Attacks -- Modern Cryptography -- Superscalar Processors, Cache Memories, and Branch Predictors -- Time-Driven Cache Attacks -- Advanced Time-Driven Cache Attacks on Block Ciphers -- A Formal Analysis of Time-Driven Cache Attacks -- Profiled Time-Driven Cache Attacks on Block Ciphers -- Access-Driven Cache Attacks on Block Ciphers -- Branch Prediction Attacks -- Countermeasures for Timing Attacks.
Sommario/riassunto	This book deals with timing attacks on software implementations of encryption algorithms. It describes and analyzes various unintended covert timing channels that are formed when ciphers are executed in microprocessors. Modern superscalar microprocessors are considered, which are enabled with features such as multi-threaded, pipelined, parallel, speculative, and out-of-order execution. Various timing attack algorithms are described and analyzed for block ciphers as well as public-key ciphers. The interplay between the cipher implementation,

system architecture, and the attack's success is analyzed. Further hardware and software countermeasures are discussed with the aim of illustrating methods to build systems that can protect against these attacks. Discusses various timing attack algorithms in detail allowing readers to reconstruct the attack. Provides several experimental results to support the theoretical analysis provided in the book. Analyzes information leakage from cache memories and branch prediction units in the processor. Examines information leakage models that would help quantify leakage in a covert timing channels.