1. Record Nr. UNINA9910482966403321

Titolo	Fault diagnosis and tolerance in cryptography : third international workshop, FDTC 2006, Yokohama, Japan, October 10, 2006 : proceedings / / Luca Breveglieri ... [et al.] (eds.)
Pubbl/distr/stampa	Berlin, : Springer, c2006
ISBN	3-540-46251-1
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XIV, 258 p.)
Collana	LNCS sublibrary. SL 4, Security and cryptology Lecture notes in computer science, , 0302-9743 ; ; 4236
Altri autori (Persone)	BreveglieriLuca
Disciplina	005.820151
Soggetti	Fault-tolerant computing Cryptography Data encryption (Computer science) - Mathematical models
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Attacks on Public Key Systems -- Is It Wise to Publish Your Public RSA Keys? -- Wagner's Attack on a Secure CRT-RSA Algorithm Reconsidered -- Attacking Right-to-Left Modular Exponentiation with Timely Random Faults -- Sign Change Fault Attacks on Elliptic Curve Cryptosystems -- Cryptanalysis of Two Protocols for RSA with CRT Based on Fault Infection -- Protection of Public Key Systems -- Blinded Fault Resistant Exponentiation -- Incorporating Error Detection in an RSA Architecture -- Data and Computational Fault Detection Mechanism for Devices That Perform Modular Exponentiation -- Attacks on and Protection of Symmetric Key Systems -- Case Study of a Fault Attack on Asynchronous DES Crypto-Processors -- A Fault Attack Against the FOX Cipher Family -- Fault Based Collision Attacks on AES -- An Easily Testable and Reconfigurable Pipeline for Symmetric Block Ciphers -- Models for Fault Attacks on Cryptographic Devices -- An Adversarial Model for Fault Analysis Against Low-Cost Cryptographic Devices -- Cryptographic Key Reliable Lifetimes: Bounding the Risk of Key Exposure in the Presence of Faults -- A Comparative Cost/Security Analysis of Fault Attack Countermeasures -- Fault-Resistant Arithmetic for Cryptography -- Non-linear Residue Codes for Robust Public-Key Arithmetic -- Fault Attack Resistant Cryptographic Hardware with

Uniform Error Detection -- Robust Finite Field Arithmetic for Fault-Tolerant Public-Key Cryptography -- Fault Attacks and Other Security Threats -- DPA on Faulty Cryptographic Hardware and Countermeasures -- Fault Analysis of DPA-Resistant Algorithms -- Java Type Confusion and Fault Attacks.

Sommario/riassunto

In recent years applied cryptography has developed considerably to satisfy the - creasing security requirements of various information technology disciplines, such as telecommunications, networking, database systems, mobile applications and others. Cryptosystems are inherently computationally complex and in order to satisfy the high throughput requirements of many applications, they are often implemented by means of either VLSI devices (cryptographic accelerators) or highly optimized software routines (cryptographic libraries) and are used via suitable (network) protocols. The sophistication of the underlying cryptographic algorithms, the high complexity of the implementations, and the easy access and low cost of cryptographic devices resulted in increased concerns regarding the reliability and security of crypto-devices. The effectiveness of side channel attacks on cryptographic devices, like timing and power-based attacks, has been known for some time. Several recent investigations have demonstrated the need to develop methodologies and techniques for designing robust cryptographic systems (both hardware and software) to protect them against both accidental faults and maliciously injected faults with the purpose of extracting the secret key. This trend has been particularly motivated by the fact that the equipment needed to carry out a successful side channel attack based on fault injection is easily accessible at a relatively low cost (for example, laser beam technology), and that the skills needed to use it are quite common. The identification of side channel attacks based on fault injections and the development of appropriate counter-measures have therefore become an active field of scientific and industrial research.