1.	Record Nr.	UNINA9910483369703321
	Titolo	Smart Card Research and Advanced Applications : 9th IFIP WG 8.8/11.2 International Conference, CARDIS 2010, Passau, Germany, April 14-16, 2010, Proceedings / / edited by Dieter Gollmann, Jean-Louis Lanet, Julien Iguchi-Cartigny
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2010
	ISBN	1-280-38627-4 9786613564191 3-642-12510-7
	Edizione	[1st ed. 2010.]
	Descrizione fisica	1 online resource (X, 239 p. 78 illus.)
	Collana	Security and Cryptology, , 2946-1863 ; ; 6035
	Altri autori (Persone)	GollmannDieter LanetJean-Louis Iguchi-CartignyJulien
	Disciplina	004.6
	Soggetti	Computer networks User interfaces (Computer systems) Human-computer interaction Computers and civilization Cryptography Data encryption (Computer science) Electronic data processing - Management Algorithms Computer Communication Networks User Interfaces and Human Computer Interaction Computers and Society Cryptology IT Operations
	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	Mathematical Algorithms -- The Polynomial Composition Problem in (? /n?)[X] -- Enhance Multi-bit Spectral Analysis on Hiding in Temporal

Dimension -- Secure Delegation of Elliptic-Curve Pairing -- Side Channel Analysis -- Side-Channel Leakage across Borders -- Designing a Side Channel Resistant Random Number Generator -- Simple Power Analysis on Exponentiation Revisited -- Atomicity Improvement for Elliptic Curve Scalar Multiplication -- Systems -- Key-Study to Execute Code Using Demand Paging and NAND Flash at Smart Card Scale -- Firewall Mechanism in a User Centric Smart Card Ownership Model -- Logical Attacks -- Combined Attacks and Countermeasures -- Attacks on Java Card 3.0 Combining Fault and Logical Attacks -- Fault Analysis -- Improved Fault Analysis of Signature Schemes -- When Clocks Fail: On Critical Paths and Clock Faults -- Privacy -- Modeling Privacy for Off-Line RFID Systems -- Developing Efficient Blinded Attribute Certificates on Smart Cards via Pairings -- On the Design and Implementation of an Efficient DAA Scheme.

Sommario/riassunto

Theseproceedingscontainthepapersselectedforpresentationat CARDIS 2010, the 9th IFIP Conference on Smart Card Research and Advanced Application hosted by the Institute of IT-Security and Security Law (ISL) of the University ofPassau,Germany. CARDISisorganizedbyIFIPWorkingGroupsWG8.8and WG 11.2. Since 1994, CARDIS has been the foremost international conference dedicated to smart card research and applications. Every second year leading researchers and practitioners meet to present new ideas and discuss recent - velopments in smart card technologies. Thefastevolutioninthe'eldofinformationsecurityrequiresadequatemeans for representing the user in human-machine interactions. Smart cards, and by extension smart devices with their processing power and their direct association with the user, are considered the ?rst choice for this purpose. A wide range of areas including hardware design, operating systems, systems modelling, cr- tography, and distributed systems contribute to this fast-growing technology. The submissions to CARDIS were reviewed by at least three members of the ProgramCommittee, followedbyatwo-weekdiscussionphaseheldelectronically, wherecommittee memberscouldcomment onall papersand allreviews. Finally, 16 papers were selected for presentation at CARDIS. There aremany volunteerswho o'ered their time and energy to put together the symposium and who deserve our acknowledgment. We want to thank all the members of the Program Committee and the external reviewers for their hard work in evaluating and discussing the submissions. We are also very grateful to JoachimPosegga,the GeneralChairof CARDIS 2010,andhisteam for thelocal conference management. Last, but certainly not least, our thanks go to all the authors who submitted papers and all the attendees. We hope you ?nd the proceedings stimulating.