1.	Record Nr.	UNINA9910484158503321
	Titolo	Foundations and Applications of Security Analysis : Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security, ARSPA-WITS 2009, York, UK, March 28-29, 2009, Revised Selected Papers / / edited by Pierpaolo Degano, Luca Viganò
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009
	ISBN	3-642-03459-4
	Edizione	[1st ed. 2009.]
	Descrizione fisica	1 online resource (X, 223 p.)
	Collana	Security and Cryptology, , 2946-1863 ; ; 5511
	Altri autori (Persone)	DeganoPierpaolo <1950-> ViganoLuca
	Disciplina	005.8
	Soggetti	Cryptography Data encryption (Computer science) Data structures (Computer science) Information theory Coding theory Computer networks Algorithms Computer engineering Cryptology Data Structures and Information Theory Coding and Information Theory Computer Communication Networks Computer Engineering and Networks
	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	A Policy Model for Secure Information Flow -- A General Framework for Nondeterministic, Probabilistic, and Stochastic Noninterference -- Validating Security Protocols under the General Attacker -- Usage Automata -- Static Detection of Logic Flaws in Service-Oriented Applications -- Improving the Semantics of Imperfect Security -- Analysing PKCS#11 Key Management APIs with Unbounded Fresh Data

-- Transformations between Cryptographic Protocols -- Formal Validation of OFEPSP+ with AVISPA -- On the Automated Correction of Protocols with Improper Message Encoding -- Finite Models in FOL-Based Crypto-Protocol Verification -- Towards a Type System for Security APIs -- Separating Trace Mapping and Reactive Simulatability Soundness: The Case of Adaptive Corruption -- How Many Election Officials Does It Take to Change an Election?.

| Sommario/riassunto | This book constitutes the thoroughly refereed post-conference proceedings of the Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security, ARSPA-WITS 2009, held in York, UK, in March 2009, in association with ETAPS 2009. The 12 revised full papers presented together with 2 invited talks were carefully reviewed and selected from 27 submissions. The papers feature topics including formal specification, analysis and design of security protocols and their applications, the formal definition of various aspects of security such as access control mechanisms, mobile code security and denial-of-service attacks, the modeling of information flow and its application to confidentiality policies, system composition and covert channel analysis. |