1. Record Nr. UNINA9910781756303321

Titolo	Formal models and techniques for analyzing security protocols [[electronic resource] /] / edited by Veronique Cortier and Steve Kremer
Pubbl/distr/stampa	Washington, D.C., : IOS Press, 2011
ISBN	6613289612 1-283-28961-X 9786613289612 1-60750-714-5
Descrizione fisica	1 online resource (312 p.)
Collana	Cryptology and information security series, , 1871-6431 ; ; v. 5
Altri autori (Persone)	CortierVeronique KremerSteve
Disciplina	005.8
Soggetti	Computer security
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 and index.
Nota di contenuto	Title page; Preface; Contents; Introduction; Verifying a Bounded Number of Sessions and Its Complexity; Constraint Solving Techniques and Enriching the Model with Equational Theories; Analysing Security Protocols Using CSP; Using Horn Clauses for Analyzing Security Protocols; Applied pi Calculus; Types for Security Protocols; Protocol Composition Logic; Shapes: Surveying Crypto Protocol Runs; Security Analysis Using Rank Functions in CSP; Computational Soundness - The Case of Diffie-Hellman Keys; Author Index
Sommario/riassunto	Security protocols are the small distributed programs which are omnipresent in our daily lives in areas such as online banking and commerce and mobile phones. Their purpose is to keep our transactions and personal data secure. Because these protocols are generally implemented on potentially insecure networks like the internet, they are notoriously difficult to devise. The field of symbolic analysis of security protocols has seen significant advances during the last few years. There is now a better understanding of decidability and complexity questions and successful automated tools for the pro