1. Record Nr.	UNISA996466180903316
Titolo	Foundations of Security, Protocols, and Equational Reasoning [[electronic resource]] : Essays Dedicated to Catherine A. Meadows / / edited by Joshua D. Guttman, Carl E. Landwehr, José Meseguer, Dusko Pavlovic
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-19052-8
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (XII, 239 p. 273 illus., 24 illus. in color.)
Collana	Security and Cryptology ; ; 11565
Disciplina	005.8
Soggetti	Data protection Computer organization Computers and civilization Software engineering Programming languages (Electronic computers) Computer logic Security Computer Systems Organization and Communication Networks Computers and Society Software Engineering Programming Languages, Compilers, Interpreters Logics and Meanings of Programs
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Cathy Meadows: A Central Figure in Protocol Analysis -- A Long, Slow Conversation -- Key Reminiscences -- Canonical Narrowing with Irreducibility Constraints as a Symbolic Protocol Analysis Method -- Finding Intruder Knowledge with Cap Matching -- Robust Declassification by Incremental Typing -- JRIF: Reactive Information Flow Control for Java -- Symbolic Timed Trace Equivalence -- Symbolic Analysis of Identity-Based Protocols -- Enrich-by-Need Protocol Analysis for Diffie-Hellman -- Key Agreement via Protocols -- Privacy

protocols -- A Multiset Rewriting Model for Specifying and Verifying Timing Aspects of Security Protocols -- Belenios: A Simple Private and Verifiable Electronic Voting System.

Sommario/riassunto

This Festschrift volume is published in honor of Catherine A. Meadows and contains essays presented at the Catherine Meadows Festschrift Symposium held in Fredericksburg, VA, USA, in May 2019. Catherine A. Meadows has been a pioneer in developing symbolic formal verification methods and tools. Her NRL Protocol Analyzer, a tool and methodology that embodies symbolic model checking techniques, has been fruitfully applied to the analysis of many protocols and protocol standards and has had an enormous influence in the field. She also developed a new temporal logic to specify protocol properties, as well as new methods for analyzing various kinds of properties beyond secrecy such as authentication and resilience under Denial of Service (DoS) attacks and has made important contributions in other areas such as wireless protocol security, intrusion detection, and the relationship between computational and symbolic approaches to cryptography. This volume contains 14 contributions authored by researchers from Europe and North America. They reflect on the long-term evolution and future prospects of research in cryptographic protocol specification and verification. .