1.	Record Nr.	UNISA996465789803316
	Titolo	Security Protocols [[electronic resource]] : 8th International Workshops Cambridge, UK, April 3-5, 2000 Revised Papers / / edited by Bruce Christianson, Bruno Crispo, James A. Malcolm, Michael Roe
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2001
	ISBN	3-540-44810-1
	Edizione	[1st ed. 2001.]
	Descrizione fisica	1 online resource (VIII, 264 p.)
	Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2133
	Disciplina	005.8
	Soggetti	Computer security Data encryption (Computer science) Computer communication systems Algorithms Management information systems Computer science Information technology Business—Data processing Systems and Data Security Cryptology Computer Communication Networks Algorithm Analysis and Problem Complexity Management of Computing and Information Systems IT in Business
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Includes index.
	Nota di contenuto	Keynote Address: Security Protocols and the Swiss Army Knife -- Mergers and Principals -- Mergers and Principals -- Authentication and Naming -- Users and Trust in Cyberspace -- Users and Trust in Cyberspace -- Interactive Identification Protocols -- Open Questions -- Looking on the Bright Side of Black-Box Cryptography -- Government Access to Keys - Panel Discussion -- Making Sense of Specifications: The Formalization of SET -- Making Sense of Specifications: The

Formalization of SET -- Lack of Explicitness Strikes Back -- Lack of Explicitness Strikes Back -- Review and Revocation of Access Privileges Distributed with PKI Certificates -- Review and Revocation of Access Privileges Distributed with PKI Certificates -- The Correctness of Crypto Transaction Sets -- The Correctness of Crypto Transaction Sets -- Micro-management of Risk in a Trust-Based Billing System -- Broadening the Scope of Fault Tolerance within Secure Services -- Broadening the Scope of Fault Tolerance within Secure Services -- DOS-Resistant Authentication with Client Puzzles -- DOS-Resistant Authentication with Client Puzzles -- Public-Key Crypto-systems Using Symmetric-Key Crypto-algorithms -- Public-Key Crypto-systems Using Symmetric-Key Crypto-algorithms -- Denial of Service — Panel Discussion -- The Resurrecting Duckling — What Next? -- The Resurrecting Duckling — What Next? -- An Anonymous Auction Protocol Using “Money Escrow” -- Short Certification of Secure RSA Modulus -- Authenticating Web-Based Virtual Shops Using Signature-Embedded Marks — A Practical Analysis — -- Authentication Web-Based Virtual Shops Using Signature-Embedded Marks — A Practical Analysis — -- I Cannot Tell a Lie -- Afterward.

Sommario/riassunto

The Cambridge International Workshop on Security Protocols has now run for eight years. Each year we set a theme, focusing upon a speci?c aspect of security protocols, and invite position papers. Anybody is welcome to send us a position paper (yes, you are invited) and we don’t insist they relate to the current theme in an obvious way. In our experience, the emergence of the theme as a unifying threadtakesplaceduringthediscussionsattheworkshopitself. Theonlyground rule is that position papers should formulate an approach to some unresolved issues, rather than being a description of a ?nished piece of work. Whentheparticipantsmeet, wetrytofocusthediscussionsupontheconc- tual issues which emerge. Security protocols link naturally to many other areas of Computer Science, and deep water can be reached very quickly. Afterwards, we invite participants to re-draft their position papers in a way which exposes the emergent issues but leaves open the way to their further development. We also prepare written transcripts of the recorded discussions. These are edited (in some cases very heavily) to illustrate the way in which the di?erent arguments and perspectives have interacted. We publish these proceedings as an invitation to the research community. Although many interesting results ?rst see the light of day in a volume of our proceedings, laying claim to these is not our primary purpose of publication. Rather, we bring our discussions and insights to a wider audience in order to suggest new lines of investigation which the community may fruitfully pursue.