

1. Record Nr.	UNISA996465831503316
Titolo	Advances in Cryptology — CRYPTO' 95
Pubbl/distr/stampa	Springer Berlin Heidelberg
Descrizione fisica	1 online resource (xii, 466 p.) : ill
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Sommario/riassunto	<p>The Crypto '95 conference was sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy, and the Computer Science Department of the University of California, Santa Barbara. It took place at the University of California, Santa Barbara, from August 27-31, 1995. This was the fifteenth annual Crypto conference; all have been held at UCSB. For the second time, proceedings were available at the conference. The General Chair, Stafford Tavares, was responsible for local organization and registration. The Program Committee considered 151 papers and selected 36 for presentation. There were also two invited talks. Robert Morris, Sr. gave a talk on "Ways of Losing Information," which included some non-cryptographic means of leaking secrets that are often overlooked by cryptographers. The second talk, "Cryptography - Myths and Realities," was given by Adi Shamir, this year's IACR Distinguished Lecturer. Shamir is the second person to receive this honor, the first having been Gus Simmons at Crypto '94. These proceedings contain revised versions of the 36 contributed talks. Each paper was sent to at least three members of the program committee for comments. Revisions were not checked on their scientific aspects. Some authors will write final versions of their papers for publication in refereed journals. Of course, the authors bear full responsibility for the contents of their papers.</p>

