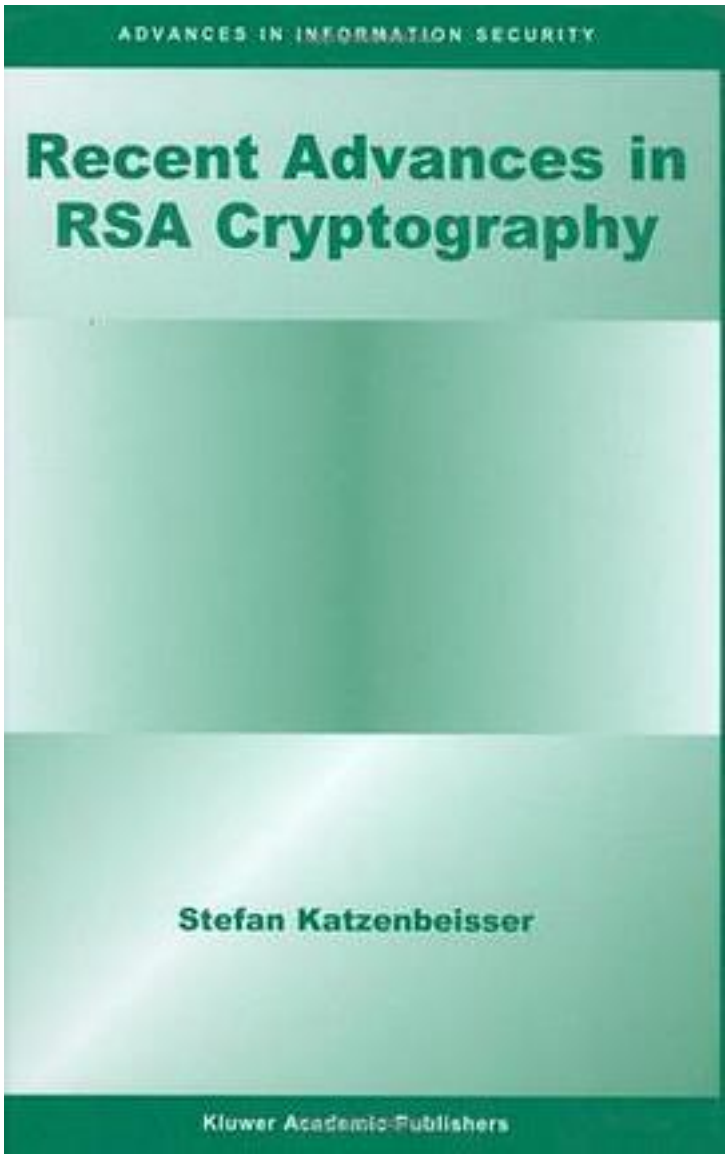
Recent Advances in RSA Cryptography (Advances in Information Security)



Recent Advances in RSA Cryptography (Advances in Information Security)_下载链接1_

著者:Stefan Katzenbeisser

出版者:Springer

出版时间:2001-09-15

装帧:Hardcover

isbn:9780792374381

Recent Advances in RSA Cryptography surveys the most important achievements of the last 22 years of research in RSA cryptography. Special emphasis is laid on the description and analysis of proposed attacks against the RSA cryptosystem. The first chapters introduce the necessary background information on number theory, complexity and public key cryptography. Subsequent chapters review factorization algorithms and specific properties that make RSA attractive for cryptographers. Most recent attacks against RSA are discussed in the third part of the book (among them attacks against low-exponent RSA, Hastad's broadcast attack, and Franklin-Reiter attacks). Finally, the last chapter reviews the use of the RSA function in signature schemes. Recent Advances in RSA Cryptography is of interest to graduate level students and researchers who will gain an insight into current research topics in the field and an overview of recent results in a unified way. Recent Advances in RSA Cryptography is suitable as a secondary text for a graduate level course, and as a reference for researchers and practitioners in industry.

作者介绍:

目录:

标签

评论

Recent Advances in RSA Cryptography (Advances in Information Security)_下载链接1_

书评

Recent Advances in RSA Cryptography (Advances in Information Security)_下载链接1_