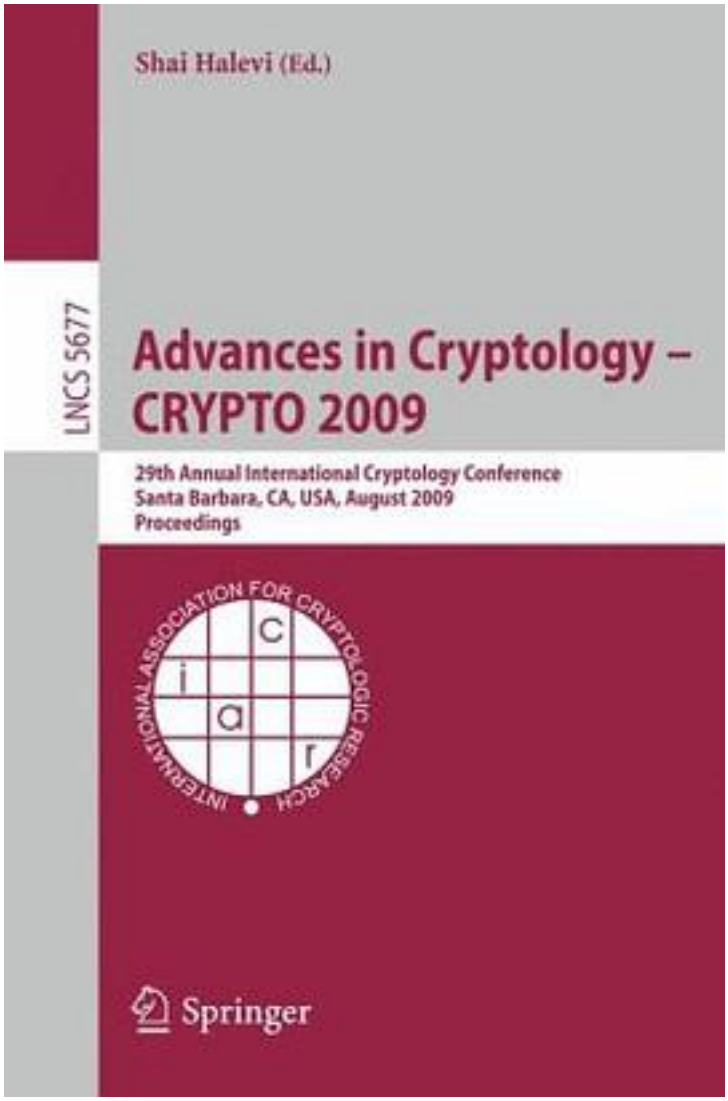
Advances in Cryptology - CRYPTO 2009



Advances in Cryptology - CRYPTO 2009_下载链接1_

著者:Halevi, Shai 编

出版者:

出版时间:

装帧:

isbn:9783642033551

This book constitutes the refereed proceedings of the 29th Annual International Cryptology Conference, CRYPTO 2009, held in Santa Barbara, CA, USA in August 2009. The 38 revised full papers presented were carefully reviewed and selected from 213 submissions. Addressing all current foundational, theoretical and research aspects of cryptology, cryptography, and cryptanalysis as well as advanced applications, the papers are organized in topical sections on key leakage, hash-function cryptanalysis, privacy and anonymity, interactive proofs and zero-knowledge, block-cipher cryptanalysis, modes of operation, elliptic curves, cryptographic hardness, merkle puzzles, cryptography in the physical world, attacks on signature schemes, secret sharing and secure computation, cryptography and game-theory, cryptography and lattices, identity-based encryption and cryptographersa (TM) toolbox.

作者介绍:

目录:

标签

评论

Advances in Cryptology - CRYPTO 2009_下载链接1_

书评

Advances in Cryptology - CRYPTO 2009_下载链接1_