Advances in cryptology – CRYPTO 2012 : 32nd Annual Cryptology Conference Santa Barbara, CA, USA, August 19-23, 2012. Proceedings

---

Abstrak

This book constitutes the refereed proceedings of the 32nd Annual International Cryptology Conference, CRYPTO 2012, held in Santa Barbara, CA, USA, in August 2012. The 48 revised full papers presented were carefully reviewed and selected from 225 submissions. The volume also contains the abstracts of two invited talks. The papers are organized in topical sections on symmetric cryptosystems, secure computation, attribute-based and functional encryption, proofs systems, protocols, hash functions, composable security, privacy, leakage and side-channels, signatures, implementation analysis, black-box separation, cryptanalysis, quantum cryptography, and key encapsulation and one-way functions.