

Public key cryptography–PKC 2012 : 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012 : proceedings

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=20410303&lokasi=lokal>

Abstrak

This book constitutes the refereed proceedings of the 15th International Conference on Practice and Theory in Public Key Cryptography, PKC 2012, held in Darmstadt, Germany, in May 2012. The 41 papers presented were carefully reviewed and selected from 188 submissions. The book also contains one invited talk. The papers are organized in the following topical sections: homomorphic encryption and LWE, signature schemes, code-based and multivariate crypto, public key encryption, special properties, identity-based encryption, public-key encryption: constructions, secure two-party and multi-party computations, key exchange and secure sessions, public-key encryption: relationships, DL, DDH, and more number theory, and beyond ordinary signature schemes.