Advances in Cryptology – EUROCRYPT 2012 : 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques Cambridge, UK, April 15-19, 2012 : proceedings

David Pointcheval, editor

Abstrak

This book constitutes the refereed proceedings of the 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2012, held in Cambgridge, UK, in April 2012.

The 41 papers, presented together with 2 invited talks, were carefully reviewed and selected from 195 submissions. The papers are organized in topical sections on index calculus, symmetric constructions, secure computation, protocols, lossy trapdoor functions, tools, symmetric cryptanalysis, fully homomorphic encryption, asymmetric cryptanalysis, efficient reductions, public-key schemes, security models, and lattices.