1. **Record Nr.**　　　　　UNINA9910484861703321

   Titolo　　　　　　　Advances in Cryptology – EUROCRYPT 2017 : 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 – May 4, 2017, Proceedings, Part III / / edited by Jean-Sébastien Coron, Jesper Buus Nielsen

   Pubbl/distr/stampa　Cham : , : Springer International Publishing : , : Imprint : Springer, , 2017

   ISBN　　　　　　　3-319-56617-2

   Edizione　　　　　[1st ed. 2017.]

   Descrizione fisica　1 online resource (XXI, 641 p. 54 illus.)

   Collana　　　　　　Security and Cryptology ; ; 10212

   Disciplina　　　　　005.82

   Soggetti　　　　　　Data encryption (Computer science)
   Computer security
   Management information systems
   Computer science
   Software engineering
   Computer science—Mathematics
   Cryptology
   Systems and Data Security
   Management of Computing and Information Systems
   Software Engineering
   Discrete Mathematics in Computer Science

   Lingua di pubblicazione　Inglese

   Formato　　　　　　Materiale a stampa

   Livello bibliografico　Monografia

   Nota di contenuto　Lattice attacks and constructions -- Obfuscation and functional encryption -- Discrete logarithm -- Multiparty computation -- Universal composability -- Zero knowledge -- Side-channel attacks and countermeasures -- Functional encryption -- Elliptic curves -- Symmetric cryptanalysis -- Provable security for symmetric cryptography -- security models:- Blockchain -- Memory hard functions -- Symmetric-key constructions -- Obfuscation -- Quantum cryptography -- Public-key encryption and key-exchange.

   Sommario/riassunto　The three-volume proceedings LNCS 10210-10212 constitute the

thoroughly refereed proceedings of the 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2017, held in Paris, France, in April/May 2017. The 67 full papers included in these volumes were carefully reviewed and selected from 264 submissions. The papers are organized in topical sections named: lattice attacks and constructions; obfuscation and functional encryption; discrete logarithm; multiparty computation; universal composability; zero knowledge; side-channel attacks and countermeasures; functional encryption; elliptic curves; symmetric cryptanalysis; provable security for symmetric cryptography; security models; blockchain; memory hard functions; symmetric-key constructions; obfuscation; quantum cryptography; public-key encryption and key-exchange.