

| | |
|-------------------------|--|
| 1. Record Nr. | UNINA9910881090403321 |
| Titolo | Advances in Cryptology – CRYPTO 2024 : 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2024, Proceedings, Part IX // edited by Leonid Reyzin, Douglas Stebila |
| Pubbl/distr/stampa | Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024 |
| ISBN | 9783031684005 9783031683992 |
| Edizione | [1st ed. 2024.] |
| Descrizione fisica | 1 online resource (509 pages) |
| Collana | Lecture Notes in Computer Science, , 1611-3349 ; ; 14928 |
| Disciplina | 005.8 |
| Soggetti | Cryptography Data encryption (Computer science) Computer engineering Computer networks Computer networks - Security measures Coding theory Information theory Cryptography Computer Engineering and Networks Mobile and Network Security Coding and Information Theory Computer Communication Networks |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Nota di bibliografia | Includes bibliographical references and index. |
| Nota di contenuto | Digital signatures -- Cloud cryptography -- Consensus protocols -- Key exchange -- Public key encryption -- Public-key cryptography with advanced functionalities -- Time-lock cryptography -- Symmetric cryptanalysis -- Symmetric cryptograph -- Mathematical assumptions -- Secret sharing -- Theoretical foundations -- Cryptanalysis -- New primitives -- Side-channels and leakage -- Quantum cryptography -- Threshold cryptography -- Multiparty computation -- Private information retrieval -- Zero-knowledge -- Succinct arguments. |
| Sommario/riassunto | The 10-volume set, LNCS 14920-14929 constitutes the refereed |

proceedings of the 44th Annual International Cryptology Conference, CRYPTO 2024. The conference took place at Santa Barbara, CA, USA, during August 18-22, 2024. The 143 full papers presented in the proceedings were carefully reviewed and selected from a total of 526 submissions. The papers are organized in the following topical sections: Part I: Digital signatures; Part II: Cloud cryptography; consensus protocols; key exchange; public key encryption; Part III: Public-key cryptography with advanced functionalities; time-lock cryptography; Part IV: Symmetric cryptanalysis; symmetric cryptograph; Part V: Mathematical assumptions; secret sharing; theoretical foundations; Part VI: Cryptanalysis; new primitives; side-channels and leakage; Part VII: Quantum cryptography; threshold cryptography; Part VIII: Multiparty computation; Part IX: Multiparty computation; private information retrieval; zero-knowledge; Part X: Succinct arguments. .
