

1. Record Nr.	UNISA996465492003316
Titolo	Advances in Cryptology – ASIACRYPT 2016 [[electronic resource]] : 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II / / edited by Jung Hee Cheon, Tsuyoshi Takagi
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2016
ISBN	3-662-53890-3
Edizione	[1st ed. 2016.]
Descrizione fisica	1 online resource (XXIV, 1055 p. 198 illus.)
Collana	Security and Cryptology ; ; 10032
Disciplina	005.824
Soggetti	Data encryption (Computer science) Computer security Coding theory Information theory Management information systems Computer science Computers Computer science—Mathematics Cryptology Systems and Data Security Coding and Information Theory Management of Computing and Information Systems Theory of Computation Mathematics of Computing
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Mathematical Analysis -- AES and White-Box -- Hash Function; Randomness -- Authenticated Encryption -- Block Cipher -- SCA and Leakage Resilience -- Zero Knowledge -- Post Quantum Cryptography -- Provable Security -- Digital Signature -- Functional and Homomorphic Cryptography -- ABE and IBE -- Foundation --

Cryptographic Protocol -- Multi-Party Computation.

Sommario/riassunto

The two-volume set LNCS 10031 and LNCS 10032 constitutes the refereed proceedings of the 22nd International Conference on the Theory and Applications of Cryptology and Information Security, ASIACRYPT 2016, held in Hanoi, Vietnam, in December 2016. The 67 revised full papers and 2 invited talks presented were carefully selected from 240 submissions. They are organized in topical sections on Mathematical Analysis; AES and White-Box; Hash Function; Randomness; Authenticated Encryption; Block Cipher; SCA and Leakage Resilience; Zero Knowledge; Post Quantum Cryptography; Provable Security; Digital Signature; Functional and Homomorphic Cryptography; ABE and IBE; Foundation; Cryptographic Protocol; Multi-Party Computation.

2. Record Nr.

UNISA996691673403316

Autore

Manulis Mark

Titolo

Applied Cryptography and Network Security Workshops : ACNS 2025 Satellite Workshops: AIHWS, AIoTS, QSHC, SCI, PrivCrypt, SPIQE, SiMLA, and CIMSS 2025, Munich, Germany, June 23–26, 2025, Revised Selected Papers, Part III // edited by Mark Manulis

Pubbl/distr/stampa

Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2026

ISBN

3-032-01823-4

Edizione

[1st ed. 2026.]

Descrizione fisica

1 online resource (357 pages)

Collana

Lecture Notes in Computer Science, , 1611-3349 ; ; 15655

Disciplina

621.39
004.6

Soggetti

Computer engineering
Computer networks
Computers
Cryptography
Data encryption (Computer science)
Computer networks - Security measures
Data protection
Computer Engineering and Networks
Computing Milieux
Cryptology
Mobile and Network Security
Data and Information Security

Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Sommario/riassunto	<p>This three-volume set LNCS constitutes the proceedings of several Satellite Workshops held in parallel with the 23rd International Conference on Applied Cryptography and Network Security, ACNS 2025, held in Munich, during June 2025. The 43 full papers and 9 poster papers presented in this volume were carefully reviewed and selected from 87 submissions. They stem from the following workshops: · 6th ACNS Workshop on Artificial Intelligence in Hardware Security (AIHWS 2025) · 7th ACNS Workshop on Artificial Intelligence and Industrial Internet-of-Things Security (AIoTS 2025) · First Workshop on Quantum-Safe Hybrid Cryptography (QSHC 2025) · 6th ACNS Workshop on Secure Cryptographic Implementation (SCI 2025) · First International Workshop on Foundations and Applications of Privacy- Enhancing Cryptography (PrivCrypt 2025) · First Workshop on Secure Protocol Implementations in the Quantum Era (SPIQE 2025) · 7th ACNS Workshop on Security in Machine Learning and its Applications (SiMLA 2025) · 5th ACNS Workshop on Critical Infrastructure and Manufacturing System Security (CIMSS 2025) .</p>