1. Record Nr. UNINA9910983309303321

Autore	Dabrowski Andrzej
Titolo	Number-Theoretic Methods in Cryptology : 4th International Conference, NuTMiC 2024, Szczecin, Poland, June 24–26, 2024, Revised Selected Papers / / edited by Andrzej Dbrowski, Josef Pieprzyk, Jacek Pomykaa
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	9783031823800 303182380X
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (762 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14966
Altri autori (Persone)	PieprzykJosef PomykaaJacek
Disciplina	005.824
Soggetti	Cryptography Data encryption (Computer science) Computer science - Mathematics Discrete mathematics Algorithms Number theory Software engineering Computers Cryptology Discrete Mathematics in Computer Science Number Theory Software Engineering Computing Milieux
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	-- Invited Talks. -- On the efficient representation of isogenies. -- Elliptic-curves factoring, witnesses and oracles. -- Elliptic Curves in Cryptography. -- On chains of pairing-friendly elliptic curves. -- Faster algorithms for isogeny computations over extensions of finite fields. -- Integral solutions of some systems of polynomial equations and constructing families of pairing-friendly elliptic curves with small

-value. -- Number Theory. -- Algebraic Equipage for Learning with Errors in Cyclic Division Algebras. -- From Worst to Average Case to Incremental Search Bounds of the Strong Lucas Test. -- Algebraic Structures and Public-Key Cryptography. -- A New Public Key Cryptosystem Based on the Cubic Pell Curve. -- The Case of Small Prime Numbers Versus the Okamoto-Uchiyama Cryptosystem. -- Compartment-based and Hierarchical Threshold Delegated Verifiable Accountable Subgroup Multi-signatures. -- Towards message recovery in NTRU Encryption with auxiliary data.

Sommario/riassunto

This book constitutes the refereed post-conference proceedings of the 4th International Conference on Number-Theoretic Methods in Cryptology, NuTMiC 2024, held in Szczecin, Poland, during June 24–26, 2024. The 9 full papers and 2 invited papers presented in this book were carefully reviewed and selected from 12 submissions. They were organized in topical sections as follows: invited talks; elliptic curves in cryptography; number theory; algebraic structures and public-key cryptography.