1.	Record Nr.	UNISA996465577503316
	Titolo	Post-quantum cryptography : second international workshop, PQCrypto 2008 Cincinnati, OH, USA, October 17-19, 2008 proceedings / / [edited by] Johannes Buchmann, Jintai Ding
	Pubbl/distr/stampa	Berlin, Germany ; ; New York, New York : , : Springer, , [2008] ©2008
	ISBN	3-540-88403-3
	Edizione	[1st ed. 2008.]
	Descrizione fisica	1 online resource (X, 231 p.)
	Collana	Security and Cryptology ; ; 5299
	Disciplina	005.82
	Soggetti	Cryptography Data encryption (Computer science)
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Includes index.
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	A New Efficient Threshold Ring Signature Scheme Based on Coding Theory -- Square-Vinegar Signature Scheme -- Attacking and Defending the McEliece Cryptosystem -- McEliece Cryptosystem Implementation: Theory and Practice -- Merkle Tree Traversal Revisited -- Explicit Hard Instances of the Shortest Vector Problem -- Practical-Sized Instances of Multivariate PKCs: Rainbow, TTS, and ?IC-Derivatives -- Digital Signatures Out of Second-Preimage Resistant Hash Functions -- Cryptanalysis of Rational Multivariate Public Key Cryptosystems -- Syndrome Based Collision Resistant Hashing -- Nonlinear Piece In Hand Perturbation Vector Method for Enhancing Security of Multivariate Public Key Cryptosystems -- On the Power of Quantum Encryption Keys -- Secure PRNGs from Specialized Polynomial Maps over Any -- MXL2: Solving Polynomial Equations over GF(2) Using an Improved Mutant Strategy -- Side Channels in the McEliece PKC.
	Sommario/riassunto	This book constitutes the refereed proceedings of the Second International Workshop on Post-Quantum Cryptography, PQCrypto 2008, held in Cincinnati, OH, USA, in October 2008. The 15 revised full papers presented were carefully reviewed and selected from numerous submissions. Quantum computers are predicted to break existing public key cryptosystems within the next decade. Post-quantum

cryptography is a new fast developing area, where public key schemes are studied that could resist these emerging attacks. The papers present four families of public key cryptosystems that have the potential to resist quantum computers: the code-based public key cryptosystems, the hash-based public key cryptosystems, the lattice-based public key cryptosystems and the multivariate public key cryptosystems.