1.

Record Nr.	UNINA9910255115503321
Autore	Koerrenz Ralf
Titolo	Existentialism and Education : An Introduction to Otto Friedrich Bollnow / / by Ralf Koerrenz ; edited by Norm Friesen
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Palgrave Macmillan, , 2017
ISBN	9783319486376 3319486373
Edizione	[1st ed. 2017.]
Descrizione fisica	1 online resource (XVII, 115 p.)
Disciplina	370.1
Soggetti	Education - Philosophy Philosophy of mind Self Educational Philosophy Philosophy of Education Philosophy of the Self
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	1. “What can we say with any certainty about human beings?” -- 2. From “Uncertainty” to “Deeper Understanding” -- 3. Between Lebensphilosophie and Existential Philosophy -- 4. Rationality of the Irrational -- 5. Educational Reality -- 6. Conclusions: Criticisms and Connections. .
Sommario/riassunto	This volume examines Otto Friedrich Bollnow’s philosophical approach to education, which brought Heidegger’s existentialism together with other theories of what it is to be “human.” This introduction to Bollnow's work begins with a summary of the theoretical influences that Bollnow synthesized, and goes on to outline his highly original account of experiential “educational reality”--namely, as a reality alternately “harmonious” or “broken,” but fundamentally “guided.” This book will be of value to scholars and students of education and philosophy, especially those interested in bringing larger existential questions into connection with everyday educational engagement.

2.	Record Nr.	UNINA9910143623403321
	Titolo	Advances in Cryptology - CRYPTO 2000 : 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000. Proceedings / / edited by Mihir Bellare
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2000
	ISBN	3-540-44598-6
	Edizione	[1st ed. 2000.]
	Descrizione fisica	1 online resource (XI, 543 p.)
	Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1880
	Disciplina	005.8/2
	Soggetti	Computer networks Data encryption (Computer science) Algorithms Management information systems Computer science Computer science - Mathematics Computer Communication Networks Cryptology Algorithm Analysis and Problem Complexity Management of Computing and Information Systems Computational Mathematics and Numerical Analysis
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Bibliographic Level Mode of Issuance: Monograph
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	XTR and NTRU -- The XTR Public Key System -- A Chosen-Ciphertext Attack against NTRU -- Privacy for Databases -- Privacy Preserving Data Mining -- Reducing the Servers Computation in Private Information Retrieval: PIR with Preprocessing -- Secure Distributed Computation and Applications -- Parallel Reducibility for Information-Theoretically Secure Computation -- Optimistic Fair Secure Computation -- A Cryptographic Solution to a Game Theoretic Problem -- Algebraic Cryptosystems -- Differential Fault Attacks on Elliptic Curve Cryptosystems -- Quantum Public-Key Cryptosystems -- New Public-Key Cryptosystem Using Braid Groups -- Message Authentication -- Key Recovery and Forgery Attacks on the MacDES

MAC Algorithm -- CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions -- L-collision Attacks against Randomized MACs -- Digital Signatures -- On the Exact Security of Full Domain Hash -- Timed Commitments -- A Practical and Provably Secure Coalition-Resistant Group Signature Scheme -- Provably Secure Partially Blind Signatures -- Cryptanalysis -- Weaknesses in the SL2( ) Hashing Scheme -- Fast Correlation Attacks through Reconstruction of Linear Polynomials -- Traitor Tracing and Broadcast Encryption -- Sequential Traitor Tracing -- Long-Lived Broadcast Encryption -- Invited Talk -- Taming the Adversary -- Symmetric Encryption -- The Security of All-or-Nothing Encryption: Protecting against Exhaustive Key Search -- On the Round Security of Symmetric-Key Cryptographic Primitives -- New Paradigms for Constructing Symmetric Encryption Schemes Secure against Chosen-Ciphertext Attack -- To Commit or Not to Commit -- Efficient Non-malleable Commitment Schemes -- Improved Non-committing Encryption Schemes Based on a General Complexity Assumption -- Protocols -- A Note on the Round-Complexity of Concurrent Zero-Knowledge -- An Improved Pseudo-random Generator Based on Discrete Log -- Linking Classical and Quantum Key Agreement: Is There “Bound Information”? -- Stream Ciphers and Boolean Functions -- Maximum Correlation Analysis of Nonlinear S-boxes in Stream Ciphers -- Nonlinearity Bounds and Constructions of Resilient Boolean Functions -- Almost Independent and Weakly Biased Arrays: Efficient Constructions and Cryptologic Applications.

Sommario/riassunto

This book constitutes the refereed proceedings of the 20th Annual International Cryptology Conference, CRYPTO 2000, held in Santa Barbara, CA, USA in August 2000. The 32 revised full papers presented together with one invited contribution were carefully reviewed and selected from 120 submissions. The papers are organized in topical sections on XTR and NTRU, privacy for databases, secure distributed computation, algebraic cryptosystems, message authentication, digital signatures, cryptanalysis, traitor tracing and broadcast encryption, symmetric encryption, to commit or not to commit, protocols, and stream ciphers and Boolean functions.