1. Record Nr. UNINA9910778336203321

Titolo	The mechanical mind in history / / edited by Philip Husbands, Owen Holland, and Michael Wheeler
Pubbl/distr/stampa	Cambridge, Mass. ; ; London, : MIT, ©2008
ISBN	0-262-31112-7 9786612096419 0-262-25638-X 1-282-09641-9 1-4356-3173-0
Descrizione fisica	1 online resource (469 p.)
Altri autori (Persone)	HusbandsPhil HollandOwen WheelerMichael <1960->
Disciplina	006.309
Soggetti	Artificial intelligence - History Artificial intelligence - Philosophy
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"A Bradford book."
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Contents; Preface; 1 Introduction: The Mechanical Mind; 2 Charles Babbage and the Emergence of Automated Reason; 3 D'Arcy Thompson: A Grandfather of A-Life 1; 4 Alan Turing's Mind Machines; 5 What Did Alan Turing Mean by "Machine"?; 6 The Ratio Club: A Hub of British Cybernetics; 7 From Mechanisms of Adaptation to Intelligence Amplifiers: The Philosophy of W. Ross Ashby; 8 Gordon Pask and His Maverick Machines; 9 Santiago Dreaming; 10 Steps Toward the Synthetic Method: Symbolic Information Processing and Self-Organizing Systems in Early Artificial Intelligence Modeling 11 The Mechanization of Art 12 The Robot Story: Why Robots Were Born and How They Grew Up; 13 God's Machines: Descartes on the Mechanization of Mind; 14 Why Heideggerian AI Failed and How Fixing It Would Require Making It More Heideggerian; 15 An Interview with John Maynard Smith; 16 An Interview with John Holland; 17 An Interview with Oliver Selfridge; 18 An Interview with Horace Barlow; 19 An Interview with Jack Cowan; About the Contributors; Index

Sommario/riassunto	The idea of intelligent machines has become part of popular culture. Tracing the history of the actual science of machine intelligence reveals a rich network of cross-disciplinary contributions, and the origins of ideas now central to artificial intelligence, artificial life, cognitive science and neuroscience.

2. Record Nr. UNINA9910548176203321

Titolo	Public-Key Cryptography – PKC 2022 : 25th IACR International Conference on Practice and Theory of Public-Key Cryptography, Virtual Event, March 8–11, 2022, Proceedings, Part I / / edited by Goichiro Hanaoka, Junji Shikata, Yohei Watanabe
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2022
ISBN	3-030-97121-X
Edizione	[1st ed. 2022.]
Descrizione fisica	1 online resource (655 pages)
Collana	Security and Cryptology, , 2946-1863 ; ; 13177
Disciplina	005.824
Soggetti	Cryptography Data encryption (Computer science) Computer engineering Computer networks Computer networks - Security measures Application software Software engineering Cryptology Computer Engineering and Networks Mobile and Network Security Computer and Information Systems Applications Software Engineering
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Cryptanalysis -- Multitarget decryption failure attacks and their

application to Saber and Kyber -- Post-quantum Security of Plain OAEP Transform -- On the security of OSIDH -- Time-Memory tradeoffs for large-weight syndrome decoding in ternary codes -- Syndrome Decoding Estimator -- On the Isogeny Problem with Torsion Point Information -- MPC and Secret Sharing -- Reusable Two-Round MPC from LPN -- On the Bottleneck Complexity of MPC with Correlated Randomness -- Low-Communication Multiparty Triple Generation for SPDZ from Ring-LPN -- Fast Batched DPSS and its Applications -- CNF-FSS and its Applications -- Cryptographic Protocols -- Effcient Verifiable Partially-Decryptable Commitments from Lattices and Applications -- Making Private Function Evaluation Safer, Faster, and Simpler -- Two-Round Oblivious Linear Evaluation from Learning with Errors -- Improved Constructions of Anonymous Credentials From StructurePreserving Signatures on Equivalence Classes -- Traceable PRFs: Full Collusion Resistance andActive Security -- Tools -- Radical Isogenies on Montgomery Curves -- Towards a Simpler Lattice Gadget Toolkit -- SNARKs and NIZKs -- Polynomial IOPs for Linear Algebra Relations -- A Unified Framework for Non-Universal SNARKs -- ECLIPSE: Enhanced Compiling method for Pedersen-committed zkSNARK Engines -- Rational Modular Encoding in the DCR Setting: Non-Interactive Range Proofs and Paillier-Based Naor-Yung in the Standard Model. .

Sommario/riassunto

The two-volume proceedings set LNCS 13177 and 13178 constitutes the refereed proceedings of the 25th IACR International Conference on Practice and Theory of Public Key Cryptography, PKC 2022, which took place virtually during March 7-11, 2022. The conference was originally planned to take place in Yokohama, Japan, but had to change to an online format due to the COVID-19 pandemic. The 40 papers included in these proceedings were carefully reviewed and selected from 137 submissions. They focus on all aspects of public-key cryptography, covering cryptanalysis; MPC and secret sharing; cryptographic protocols; tools; SNARKs and NIZKs; key exchange; theory; encryption; and signatures.