1. Record Nr. UNINA9911142464603321

Autore	El Mrabet Nadia
Titolo	Guide to pairing-based cryptography / / Nadia El Mrabet, SAS, Ecole des Mines de Saint Etienne, Gardanne, France, Marc Joye, NXP Semiconductors, San Jose, USA
Pubbl/distr/stampa	Boca Raton : , : CRC Press, , [2017] ©2017
ISBN	1-315-35314-8 1-315-37017-4 1-4987-2951-7 9781315370170
Edizione	[1st ed.]
Descrizione fisica	1 online resource (32 pages)
Collana	Chapman & Hall/CRC cryptography and network security issues
Disciplina	005.8/2
Soggetti	Curves, Elliptic Cryptography Sets of pairs of functions to be distinguished Data encryption (Computer science) - Mathematics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	1. Pairing-based cryptography / Sebastien Canard and Jacques Traore? -- 2. Mathematical background / Jean-Luc Beuchat, Nadia El Mrabet, Laura Fuentes-Casta/eda, and Francisco Rodriguez-Henriquez -- 3. Pairings / Sorina Ionica and Damien Robert -- 4. Pairing-friendly elliptic curves / Safia Haloui and Edlyn Teske -- 5. Arithmetic of finite fields / Jean Luc Beuchat, Luis J. Dominguez Perez, Sylvain Duquesne, Nadia El Mrabet, Laura Fuentes-Casta/eda, and Francisco Rodriguez-Henriquez -- 6. Scalar multiplication and exponentiation in pairing groups / Joppe Bos, Craig Costello, and Michael Naehrig -- 7. Final exponentiation / Jean-Luc Beuchat, Luis J. Dominguez Perez, Laura Fuentes-Castaneda, and Francsico Rodriguez-Henriquez -- 8. Hashing into elliptic curves / Eduardo Ochoa-Jimenez, Francisco Rodriguez-Henriquez, and Mehdi Tibouchi -- 9. Discrete logarithms / Aurore Guillevic and Francois Morain -- 10. Choosing parameters / Sylvain Duquesne, Nadia El Mrabet, Safia Haloui, Damien Robert, and Franck

Rondepierre -- 11. Software implementation / Diego F. Aranha, Luis J. Dominguez Perez, Amine Mrabet, and Peter Schwabe -- 12. Physical attacks / Nadia El Mrabet, Louis Goubin, Sylvain Guilley, Jacques Fournier, Damien Jauvart, Martin Moreau, Pablo Rauzy, and Franck Rondepierre.

Sommario/riassunto

This book is devoted to efficient pairing computations and implementations, useful tools for cryptographers working on topics like identity-based cryptography and the simplification of existing protocols like signature schemes. As well as exploring the basic mathematical background of finite fields and elliptic curves, Guide to Pairing-Based Cryptography offers an overview of the most recent developments in optimizations for pairing implementation. Each chapter includes a presentation of the problem it discusses, the mathematical formulation, a discussion of implementation issues, solutions accompanied by code or pseudocode, several numerical results, and references to further reading and notes. Intended as a self-contained handbook, this book is an invaluable resource for computer scientists, applied mathematicians and security professionals interested in cryptography.