1. Record Nr. UNINA9910495213803321

Autore	Safieh Malek
Titolo	Algorithms and architectures for cryptography and source coding in non-volatile flash memories / / Malek Safieh
Pubbl/distr/stampa	Wiesbaden, Germany : , : Springer Vieweg, , [2021] ©2021
ISBN	3-658-34459-8
Edizione	[1st ed. 2021.]
Descrizione fisica	1 online resource (XVI, 142 p. 26 illus., 3 illus. in color.)
Collana	Schriftenreihe der Institute Fur Systemdynamik (ISD) und Optische Systeme (IOS), , 2661-8087
Disciplina	652.8
Soggetti	Cryptography Data encryption (Computer science) Revision control (Computer science) - Mathematics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	1 Introduction -- 2 Elliptic curve cryptography -- 3 Elliptic curve cryptography over Gaussian integers -- 4 Montgomery arithmetic over Gaussian integers -- 5 Architecture of the ECC coprocessor for Gaussian integers -- 6 Compact architecture of the ECC coprocessor for binary extension fields -- 7 The parallel dictionary LZW algorithm for flash memory controllers -- 8 Conclusion.
Sommario/riassunto	In this work, algorithms and architectures for cryptography and source coding are developed, which are suitable for many resource-constrained embedded systems such as non-volatile flash memories. A new concept for elliptic curve cryptography is presented, which uses an arithmetic over Gaussian integers. Gaussian integers are a subset of the complex numbers with integers as real and imaginary parts. Ordinary modular arithmetic over Gaussian integers is computational expensive. To reduce the complexity, a new arithmetic based on the Montgomery reduction is presented. For the elliptic curve point multiplication, this arithmetic over Gaussian integers improves the computational efficiency, the resistance against side channel attacks, and reduces the memory requirements. Furthermore, an efficient variant of the Lempel-Ziv-Welch (LZW) algorithm for universal lossless data compression is investigated. Instead of one LZW dictionary, this algorithm applies

several dictionaries to speed up the encoding process. Two dictionary partitioning techniques are introduced that improve the compression rate and reduce the memory size of this parallel dictionary LZW algorithm. About the Author Malek Safieh is a research scientist in the field of cryptography and data compression.