Schriftenreihe der Institute für Systemdynamik (ISD)
und optische Systeme (IOS)

RESEARCH

Malek Safieh

Algorithms and Architectures for Cryptography and Source Coding in Non-Volatile Flash Memories

Springer Vieweg

Schriftenreihe der Institute für Systemdynamik (ISD) und optische Systeme (IOS)

Die „Schriftenreihe der Institute für Systemdynamik (ISD) und optische Systeme (IOS)“ deckt ein breites Themenspektrum ab: von angewandter Informatik bis zu Ingenieurswissenschaften. Die Institute für Systemdynamik und optische Systeme bilden gemeinsam einen Forschungsschwerpunkt der Hochschule Konstanz. Die Forschungsprogramme der beiden Institute umfassen informations- und regelungstechnische Fragestellungen sowie kognitive und bildgebende Systeme. Das Bindeglied ist dabei der Systemgedanke mit systemtechnischer Herangehensweise und damit verbunden die Suche nach Methoden zur Lösung interdisziplinärer, komplexer Probleme. In der Schriftenreihe werden Forschungsergebnisse in Form von Dissertationen veröffentlicht.

The “Series of the institutes of System Dynamics (ISD) and Optical Systems (IOS)” covers a broad range of topics: from applied computer science to engineering. The institutes of System Dynamics and Optical Systems form a research focus of the HTWG Konstanz. The research programs of both institutes cover problems in information technology and control engineering as well as cognitive and imaging systems. The connective link is the system concept and the systems engineering approach, i.e. the search for methods and solutions of interdisciplinary, complex problems. The series publishes research results in the form of dissertations.

Weitere Bände in der Reihe http://www.springer.com/series/16265

Malek Safieh

Algorithms and Architectures for Cryptography and Source Coding in Non-Volatile Flash Memories

Springer Vieweg

Malek Safieh
University of Ulm
Munich, Germany

Dissertation, Ulm University, 2021

ISSN 2661-8087 ISSN 2661-8095 (electronic)
Schriftenreihe der Institute für Systemdynamik (ISD) und optische Systeme (IOS)
ISBN 978-3-658-34458-0 ISBN 978-3-658-34459-7 (eBook)
https://doi.org/10.1007/978-3-658-34459-7

Responsible Editor: Stefanie Eggert
This Springer Vieweg imprint is published by the registered company Springer Fachmedien Wiesbaden GmbH part of Springer Nature.
The registered company address is: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Acknowledgements

First and foremost, I would like to thank my doctoral supervisor Prof. Dr. Jürgen Freudenberger for giving me the opportunity to join the research group at the Institute of System Dynamics (ISD) at the University of Applied Sciences (HTWG) Konstanz, Germany. Due to his efforts, it became possible for me to work on my Ph.D. for the last three and a half years. I appreciate the valuableness, the time, and efforts he offered for the long and fruitful discussions we had. I am very grateful for his advices and supports that contributed to the improvement of my research skills.

I would also like to thank Prof. Dr. Martin Bossert for reading my thesis and being my second supervisor. I am very thankful to all the research members at the ISD. It would be truly unfair to mention only a few people since everyone made my time there a pleasure. The conversations during the coffee breaks in the kitchen, after eating in the canteen, as well as during the after-work beer were always fun, kept me motivated and with a fresh mindset.

I would like to express my gratitude to my family and friends for all their help and contribution during my study and the research period. Further thanks goes to everyone who supported me during my doctoral research.

Abstract

Flash memory is an important non-volatile storage medium. Reliable and secure data storage in flash memories requires sophisticated coding and signal processing techniques. Although error-correcting codes are applied in practically all flash storage systems, coding techniques for cryptography and data compression are less developed.

Due to the limited computational performance of the flash controller, many flash storage systems rely on symmetric cryptography for the message authentication. Asymmetric cryptography like elliptic curve cryptographic (ECC) systems offer additional functionality such as digital signatures and key exchange methods, which allows a verification of the integrity and authenticity. In this work, we demonstrate that ECC systems over Gaussian integers are very efficient. Gaussian integers are a subset of complex numbers with integers as real and imaginary parts. Since many Gaussian integer fields are isomorphic to prime fields, this arithmetic is suitable for ECC systems. Implementations of cryptographic algorithms are prone to side channel attacks. We show that using Gaussian integers can reduce the complexity and memory requirements for hardware implementations which are protected against such attacks.

However, determining the modulo reduction over Gaussian integers is extremely expensive. To reduce the complexity, we derive a Montgomery modular arithmetic over Gaussian integers. Moreover, we develop a hardware architecture optimized for the ECC operations targeting low area. The proposed ECC processor for Gaussian integers is a competitive solution for applications in flash memories and other resource-constrained embedded systems.

Data compression provides several advantages for flash memory controllers, e.g. improving the lifetime and storage capacity. In this work, we focus on the

dictionary-based Lempel-Ziv-Welch (LZW) algorithm. A fast and compact implementation of this universal data compression procedure is a challenging task due to the recursive structure of the LZW dictionary. To speed up the encoding, we present an architecture that applies multiple dictionaries in parallel. Two dictionary partitioning techniques are introduced that improve the compression rate and reduce the memory size of this parallel dictionary LZW algorithm.

Contents

Acronyms

ADD	point addition
AES	advanced encryption standard
ANSI	American National Standards Institute
ASCII	American standard code for information interchange
ASIC	application-specific integrated circuit
ASIP	application-specific instruction set processor
BCH	Bose Chaudhuri Hocqenhem
BMH	BWT-MTF-Huffman
BWT	Burrows-Wheeler transformation
CAM	content-addressable memories
DBL	point doubling
DPA	differential power analysis
DP-RAM	dual-port RAM
DSP	digital signal processor
ECC	elliptic curve cryptographic
FF	flip-flops
FPGA	field programmable gate array
FTL	flash translation layer
GF	Galois field
HDD	hard disc drives
HMAC	keyed-hash message authentication code
KB	Kilobyte
LUT	lookup tables
LZW	Lempel-Ziv-Welch
MAC	message authentication codes
MH	MTF-Huffman

MLC	multi-level cell
MTF	move-to-front
NIST	National Institute of Standards and Technology
P/E	program/erase
PDLZW	parallel dictionary LZW
PM	elliptic curve point multiplication
RAM	random-access memory
RIP	randomized initial point
RPA	refined power analysis
RSA	Rivest-Shamir-Adleman
SADD	special point addition
SCA	side channel attacks
SD	secure digital
SPA	simple power analysis
SSD	solid-state drives
TA	timing attacks
USB	universal serial bus
WER	word error rate
ZPA	zero-value point attacks

List of Figures

List of Tables