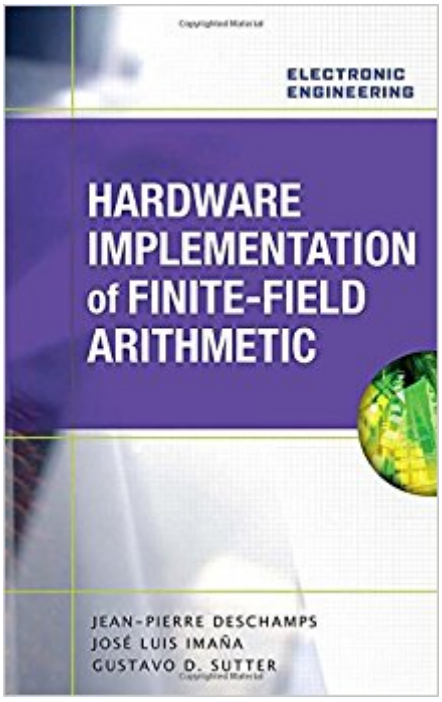
Hardware Implementation Of Finite-Field Arithmetic (Electronic Engineering)



Synopsis

Implement Finite-Field Arithmetic in Specific Hardware (FPGA and ASIC)Master cutting-edge electronic circuit synthesis and design with help from this detailed guide. Hardware Implementation of Finite-Field Arithmetic describes algorithms and circuits for executing finite-field operations, including addition, subtraction, multiplication, squaring, exponentiation, and division.This comprehensive resource begins with an overview of mathematics, covering algebra, number theory, finite fields, and cryptography. The book then presents algorithms which can be executed and verified with actual input data. Logic schemes and VHDL models are described in such a way that the corresponding circuits can be easily simulated and synthesized. The book concludes with a real-world example of a finite-field application--elliptic-curve cryptography. This is an essential guide for hardware engineers involved in the development of embedded systems. Get detailed coverage of:Modulo m reductionModulo m addition, subtraction, multiplication, and exponentiationOperations over GF(p) and GF(pm)Operations over the commutative ringÃ Â Zp[x]/f(x)Operations over the binary field GF(2m) using normal, polynomial, dual, and triangular

Book Information

Series: Electronic Engineering

Hardcover: 360 pages

Publisher: McGraw-Hill Education; 1 edition (March 12, 2009)

Language: English

ISBN-10: 0071545816

ISBN-13: 978-0071545815

Product Dimensions: 6.3 x 1.2 x 9.3 inches

Shipping Weight: 1.4 pounds (View shipping rates and policies)

Average Customer Review: 4.4 out of 5 stars 2 customer reviews

Best Sellers Rank: #2,413,458 in Books (See Top 100 in Books) #89 inÃ Â Books > Engineering & Transportation > Engineering > Electrical & Electronics > Circuits > VLSI & ULSI #257 inÃ Â Books > Computers & Technology > Hardware & DIY > Microprocessors & System Design > Embedded Systems #267 inÃ Â Books > Engineering & Transportation > Engineering > Electrical & Electronics > Circuits > Integrated

Customer Reviews

Jean-Pierre Deschamps, Ph.D., is a professor at the University Rovira i Virgili in Tarragona, Spain. JosÃƒÂ© Luis ImaÃƒÂ a, Ph.D., is a professor at Complutense University of Madrid, Spain.

Gustavo D. Sutter, Ph.D., is a professor at the Autonomous University of Madrid, Spain.

Jean-Pierre Deschamps lives in an interesting region bounded by embedded systems, math circuits, cryptography and field programmable devices. His tools of choice are FPGA, ASIC and VHDL. The intersection area of all three of his most powerful and current books is the transition from already planned algorithms to circuits. There is enough breadth and depth to provide both a reference for practicing EE's and students in these specific areas. What you don't get in any of his books are specific algorithms.Jean-Pierre uses more of a "here is the general structure of the algorithm" with practical tips on steps and stages rather than complete specs, for what I'd call "pseudo algos" much like pseudo code. However, in this case there are many details on how the basic functions TRANSLATE both to algorithms, and especially circuits, including downloadable circuit diagrams in many areas.His most important contributions include:Guide to FPGA Implementation of Arithmetic Functions (Lecture Notes in Electrical Engineering)Synthesis of Arithmetic Circuits: FPGA, ASIC and Embedded SystemsHardware Implementation of Finite-Field Arithmetic (Electronic Engineering)All three books give deep detail about the math involved itself-- citing where functions are continuous and derivable enough NEAR a computational area at which successive approximations can be processed, for example.Given the paucity of any current and recent books on math circuits, and even journal articles, Deschamps is a breath of fresh air in this space. The older books have a lot of algorithms but didn't have to cope with today's memory and parallel processing nightmares. They also didn't forsee the incredible explosion of embedded systems we're seeing today. These books are NOT cheap, and we always surf for their warehouse deals when we recommend these texts for our classpros dot com Engineering teachers. The feedback we've gotten on all three of Deschamps titles above is outstanding-- over 33 professors we've recommended these to are now actively using them in courses and especially labs.If you're looking to supercharge your professional life in the hottest new areas in ICs-- embedded systems, mobile devices and math-- Jean-Pierre's trifecta is a GREAT place to start.I'm the CTO of an Engineering Education and circuit programming firm, and have no relationship with the author, publisher, , etc. LP reviews are strictly for the benefit of readers, and we always buy the books we review or recommend to libraries and schools.

i love the product, it is very well balanced, has lot of weight to it, and it is very sharp. it cuts through bread so easily and makes perfect slices. quality. I'll be buying again. OK . very recommend . OK it is a very useful tool,

Hardware Implementation of Finite-Field Arithmetic (Electronic Engineering) The Hardware Hacker: Adventures in Making and Breaking Hardware The Finite Element Method: Linear Static and Dynamic Finite Element Analysis (Dover Civil and Mechanical Engineering) Handmade Electronic Music: The Art of Hardware Hacking Airborne Electronic Hardware Design Assurance: A Practitioner's Guide to RTCA/DO-254 How the Universe Got Its Spots: Diary of a Finite Time in a Finite Space Finite Mathematics and Calculus with Applications Plus MyMathLab with Pearson eText -- Access Card Package (10th Edition) (Lial, Greenwell & Ritchey, The Applied Calculus & Finite Math Series) Finite Mathematics Plus MyMathLab with Pearson eText -- Access Card Package (11th Edition) (Lial, Greenwell & Ritchey, The Applied Calculus & Finite Math Series) Digital Systems Design and Prototyping: Using Field Programmable Logic and Hardware Description Languages Energy Systems Engineering: Evaluation and Implementation, Third Edition (P/L Custom Scoring Survey) Energy Systems Engineering: Evaluation and Implementation, Second Edition Electronic Cigarette: The Ultimate Guide for Understanding E-Cigarettes And What You Need To Know (Vaping Pen, Electronic Hookah, E-Hookah, E-Liquid, Alternative, Juice, G-Pen, Starter Kit) Essentials of Electronic Testing for Digital, Memory and Mixed-Signal VLSI Circuits (Frontiers in Electronic Testing) Encapsulation Technologies for Electronic Applications (Materials and Processes for Electronic Applications) Handbook of Organic Materials for Optical and (Opto)Electronic Devices: Properties and Applications (Woodhead Publishing Series in Electronic and Optical Materials) IEC 61508-7 Ed. 1.0 b:2000, Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures Electronic Document Preparation and Management for CSEC Study Guide: Covers latest CSEC Electronic Document Preparation and Management syllabus. Finite Models and Methods of Dynamics in Structures (Developments in Civil Engineering) A First Course in the Finite Element Method (Activate Learning with these NEW titles from Engineering!) Finite-Dimensional Variational Inequalities and Complementarity Problems (Springer Series in Operations Research and Financial Engineering)