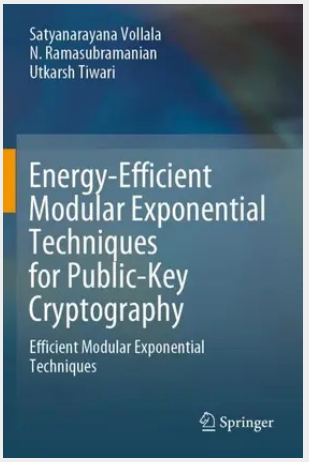
Vollala / Ramasubramanian / Tiwari

Energy-Efficient Modular Exponential Techniques for Public-Key Cryptography

Efficient Modular Exponential Techniques



Cryptographic applications, such as RSA algorithm, ElGamal cryptography, elliptic curve cryptography, Rabin cryptosystem, Diffie -Hellmann key exchange algorithm, and the Digital Signature Standard, use modular exponentiation extensively. The performance of all these applications strongly depends on the efficient implementation of modular exponentiation and modular multiplication. Since 1984, when Montgomery first introduced a method to evaluate modular multiplications, many algorithmic modifications have been done for improving the efficiency of modular multiplication, but very less work has been done on the modular exponentiation to improve the efficiency. This research monograph addresses the question- how can the performance of modular exponentiation, which is the crucial operation of many public-key cryptographic techniques, be improved?
The book focuses on Energy Efficient Modular Exponentiations for Cryptographic hardware. Spread across five chapters, this well-researched text focuses in detail on the Bit Forwarding Techniques and the corresponding hardware realizations. Readers will also discover advanced performance improvement techniques based on high radix multiplication and Cryptographic hardware based on multi-core architectures.

This unique and focused research monograph addresses the question: How can the performance of modular exponentiation, which is the crucial operation of many public-key cryptographic techniques, be improved? Cryptographic applications--such as RSA algorithms, ElGamal cryptography, elliptic-curve cryptography, Rabin cryptosystems, Diffie -Hellmann key-exchange algorithms, and the Digital Signature Standard--use modular exponentiation extensively. The performance of all these applications strongly depends on the efficient implementation of modular exponentiation and modular multiplication. Since 1984, when Montgomery first introduced a method to evaluate modular multiplications, many algorithmic modifications have been done for improving the efficiency of modular multiplication, but very less work has been done on the modular exponentiation to improve the efficiency. The book focuses on energy-efficient modular exponentiation for cryptographic hardware. Spread across five chapters, this well-researched text focuses in detail on bit forwarding techniques and the corresponding hardware realizations. Readers will also discover advanced performance-improvement techniques based on high radix multiplication and cryptographic hardware based on multi-core architectures. Satyanarayana Vollala is a full-time Ph.D. research scholar in the Department of Computer Science and Engineering at National Institute of Technology, Tiruchirappalli, Tamil Nadu, India. N. Ramasubramanian is an associate professor in the Department of Computer Science and Engineering at National Institute of Technology, Tiruchirappalli, India.

181,89 €
169,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783030745264
Medium: Buch
ISBN: 978-3-030-74526-4
Verlag: Springer International Publishing
Erscheinungstermin: 15.07.2022
Sprache(n): Englisch
Auflage: 1. Auflage 2021
Produktform: Kartoniert
Gewicht: 429 g
Seiten: 257
Format (B x H): 155 x 235 mm

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)