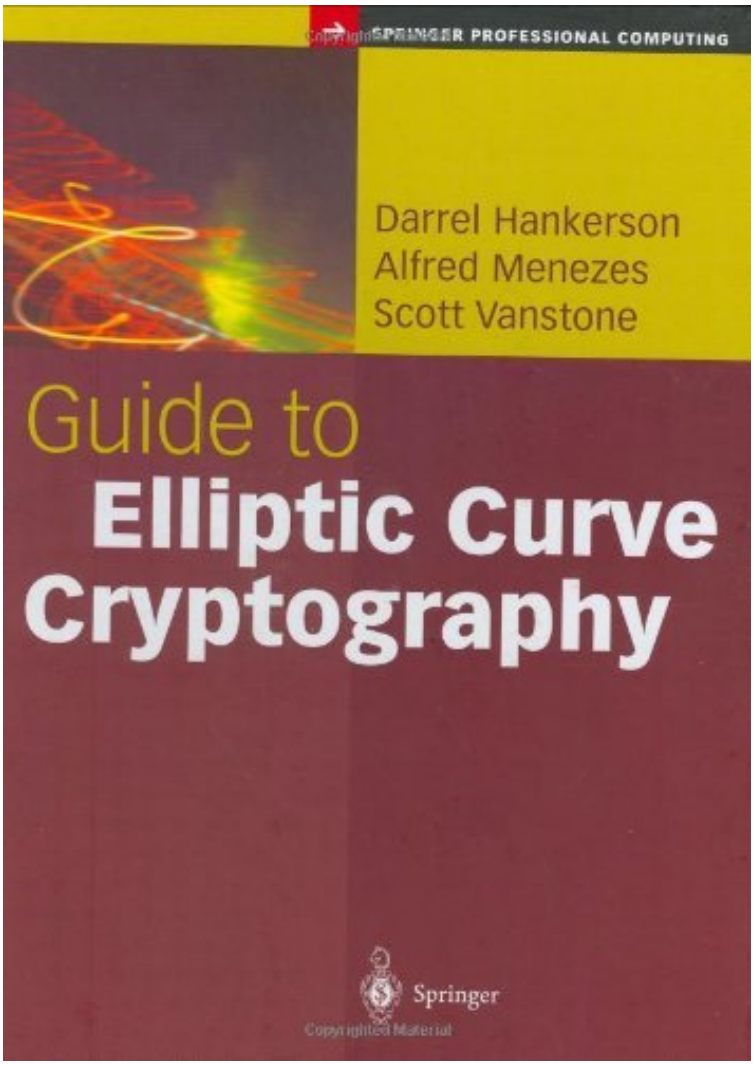
# Guide to Elliptic Curve Cryptography (Springer Professional Computing)

*Von Darrel Hankerson, Alfred J. Menezes, Scott Vanstone*
*ePub | *DOC | audiobook | ebooks | Download PDF*






Produktinformation -Verkaufsrang: #866676 in eBooksVerffentlicht am: 2006-06-01Erscheinungsdatum: 2006-06-01File Name: B000VI6S6G | File size: 37.Mb

**Von Darrel Hankerson, Alfred J. Menezes, Scott Vanstone : Guide to Elliptic Curve Cryptography (Springer Professional Computing)** before purchasing it in order to gage whether or not it would be worth my time, and all praised Guide to Elliptic Curve Cryptography (Springer Professional Computing):

KundenrezensionenHilfreichste Kundenrezensionen4 von 4 Kunden fanden die folgende Rezension hilfreich. "The Book" for ECC implementersVon Ein KundeThis is a wonderful book we all have been waiting for with the essential stuff about implementing Elliptic Curve Cryptography in both software and hardware. The authors know the real world problems when it comes down to implementation issues concerning word storage and access in processors.The

book gives a good description on all layers of the ECC implementation from field multiplication algorithms(prime, binary and also Optimal Extension fields), point multiplication(including multiple point multiplication) to different protocols for key establisment. The chapter on implementation issues makes it an all round book for implementers as an easy reference tool without getting lost in all the maths.Overall this book is just not any other book on ECC but "the book" on ECC which finds its rightful place among cryptographic system implementors.

KurzbeschreibungAfter two decades of research and development, elliptic curve cryptography now has widespread exposure and acceptance. Industry, banking, and government standards are in place to facilitate extensive deployment of this efficient public-key mechanism. Anchored by a comprehensive treatment of the practical aspects of elliptic curve cryptography (ECC), this guide explains the basic mathematics, describes state-of-the-art implementation methods, and presents standardized protocols for public-key encryption, digital signatures, and key establishment. In addition, the book addresses some issues that arise in software and hardware implementation, as well as side-channel attacks and countermeasures. Readers receive the theoretical fundamentals as an underpinning for a wealth of practical and accessible knowledge about efficient application. Features Benefits:* Breadth of coverage and unified, integrated approach to elliptic curve cryptosystems* Describes important industry and government protocols, such as the FIPS 186-2 standard from the U.S. National Institute for Standards and Technology* Provides full exposition on techniques for efficiently implementing finite-field and elliptic curve arithmetic* Distills complex mathematics and algorithms for easy understanding* Includes useful literature references, a list of algorithms, and appendices on sample parameters, ECC standards, and software toolsThis comprehensive, highly focused reference is a useful and indispensable resource for practitioners, professionals, or researchers in computer science, computer engineering, network design, and network data security.PressestimmenFrom the reviews: "It is the first book to give a comprehensive and careful presentation of all the implementation issues involved with ECC. The book contains chapters on implementing finite field arithmetic . There is also an extensive chapter on engineering considerations . is very clearly written and numerous algorithms are presented in a format suitable for easy implementations. The book will be useful for engineers and computer scientists who want to know about the important issues in implementing ECC." (Steven D. Galbraith, Mathematical s, 2005) "This book is entirely dedicated to elliptic curve cryptography. It starts after a short overview with finite field arithmetic . The book is a guide for security professionals and developers . It is very carefully written and may serve as a reference book for mathematicians as well." (J. Schoissengeier, Monatshefte fr Mathematik, Vol. 144 (1), 2005) "This is a very useful handbook for anybody who is or must be interested in practical elliptic curve cryptography and its applications. is presented in a rather non-theoretical way and at a beginner to intermediate level. On the other hand, researchers should find the book useful because of the extensive survey of the related literature (each chapter ends with notes and further references, the bibliography containing almost 500 items)." (EMS Newsletter, September, 2005)KurzbeschreibungAfter two decades of research and development, elliptic curve cryptography now has widespread exposure and acceptance. Industry, banking, and government standards are in place to facilitate extensive deployment of this efficient public-key mechanism. Anchored by a comprehensive treatment of the practical aspects of elliptic curve cryptography (ECC), this guide explains the basic mathematics, describes state-of-the-art implementation methods, and presents standardized protocols for public-key encryption, digital signatures, and key establishment. In addition, the book addresses some issues that arise in software and hardware implementation, as well as side-channel attacks and countermeasures. Readers receive the theoretical fundamentals as an underpinning for a wealth of practical and accessible knowledge about efficient application. Features Benefits:* Breadth of coverage and unified, integrated approach to elliptic curve cryptosystems* Describes important industry and government protocols, such as the FIPS 186-2 standard from the U.S. National Institute for Standards and Technology* Provides full exposition on techniques for efficiently implementing finite-field and elliptic curve arithmetic* Distills complex mathematics and algorithms for easy understanding* Includes useful literature references, a list of algorithms, and appendices on sample parameters, ECC standards, and software toolsThis comprehensive, highly focused reference is a useful and indispensable resource for practitioners, professionals, or researchers in computer science, computer engineering, network design, and network data security.