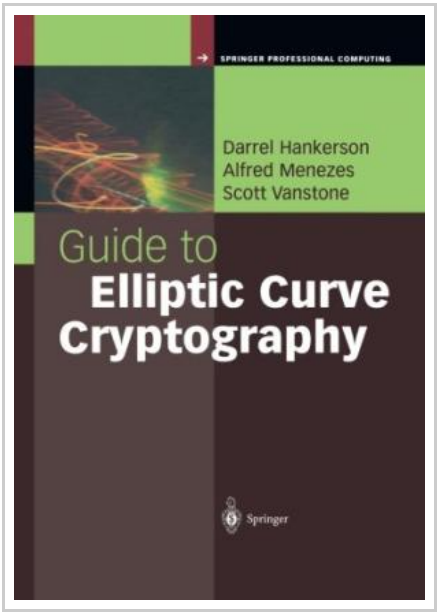

DOWNLOAD

Guide to Elliptic Curve Cryptography

By Hankerson, Darrel / Menezes, Alfred J.

Book Condition: New. Publisher/Verlag: Springer, Berlin | After 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 cryptosystemsDescribes important industry and government protocols, such as the FIPS 186-2 standard from the U.S. National Institute for Standards and TechnologyProvides full exposition on techniques for efficiently implementing finite-field and elliptic curve arithmeticDistills complex mathematics and algorithms for easy understandingIncludes 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...

Reviews

This kind of pdf is every thing and made me seeking ahead plus more. It is probably the most amazing ebook i have study. I am quickly can get a enjoyment of reading a composed pdf.

-- ***Florence Rutherford DDS***

Definitely among the best ebook I actually have possibly read through. It is really simplified but unexpected situations in the 50 % from the publication. You wont truly feel monotony at at any time of the time (that's what catalogues are for concerning in the event you ask me).

-- ***Jerald Champlin II***