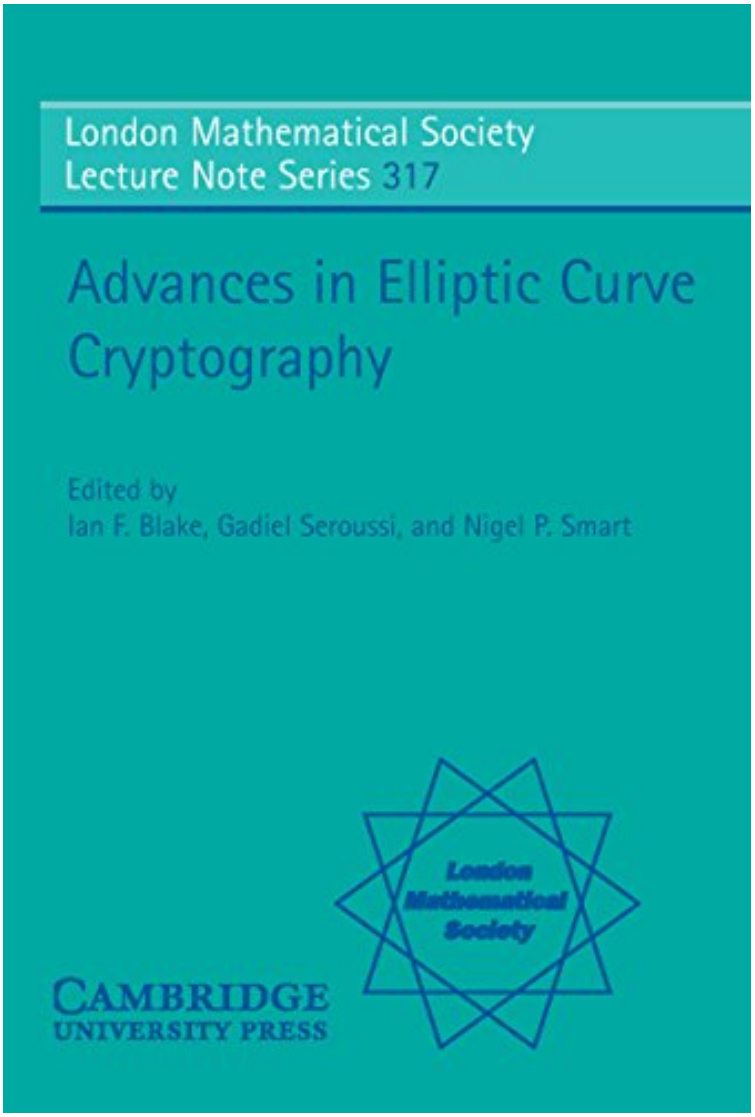
Advances in Elliptic Curve Cryptography



*De Cambridge University Press ebooks | Download PDF | *ePub | DOC | audiobook*

Dtails sur le produit Publi le: 2005-04-25Sorti le: 2005-04-25Format: Ebook Kindle

(Download pdf ebook) Advances in Elliptic Curve Cryptography

De Cambridge University Press : Advances in Elliptic Curve Cryptography before purchasing it in order to gage whether or not it would be worth my time, and all praised Advances in Elliptic Curve Cryptography:

Description :

Prsentation de l'diteurSince the appearance of the authors' first volume on elliptic curve cryptography in 1999 there has been tremendous progress in the field. In some topics, particularly point counting, the progress has been spectacular. Other topics such as the Weil and Tate pairings have been applied in new and important ways to cryptographic protocols that hold great promise. Notions such as provable security, side channel analysis and the Weil descent technique have also grown in importance. This second volume addresses these advances and brings the reader up to date. Prominent contributors to the research literature in these areas have provided articles that reflect the current state of these important topics. They are divided into the areas of protocols, implementation techniques, mathematical foundations and pairing based cryptography. Each of the topics is presented in an accessible, coherent and consistent manner for a wide

audience that will include mathematicians, computer scientists and engineers.Revue de presse' gives a comprehensive explanation of elliptic curve cryptography. It is clearly written and is appropriate for both computer scientists and mathematicians interested in the field.' E. Schaefer, Niew Archief voor Wiskunde' a very well written description of the use of elliptic curves in public key cryptography.' Franck Leprvost, Zentralblatt fr Mathematik'An excellent new book on elliptic curve theory and practical implementation.' Dr Dobb's Journal Online' a good introduction to the mathematics behind the design of elliptic-curve cryptosystems and their implementation this work is an important addition to the literature.' Jonathan Golan, Computing s' written in a very readable form and thus can be consulted and used both by mathematicians and by anybody wishing to learn more about the mathematics behind the implementations of elliptic curve cryptosystems.' European Maths Society JournalPrsentation de l'diteurSince the appearance of the authors' first volume on elliptic curve cryptography in 1999 there has been tremendous progress in the field. In some topics, particularly point counting, the progress has been spectacular. Other topics such as the Weil and Tate pairings have been applied in new and important ways to cryptographic protocols that hold great promise. Notions such as provable security, side channel analysis and the Weil descent technique have also grown in importance. This second volume addresses these advances and brings the reader up to date. Prominent contributors to the research literature in these areas have provided articles that reflect the current state of these important topics. They are divided into the areas of protocols, implementation techniques, mathematical foundations and pairing based cryptography. Each of the topics is presented in an accessible, coherent and consistent manner for a wide audience that will include mathematicians, computer scientists and engineers.