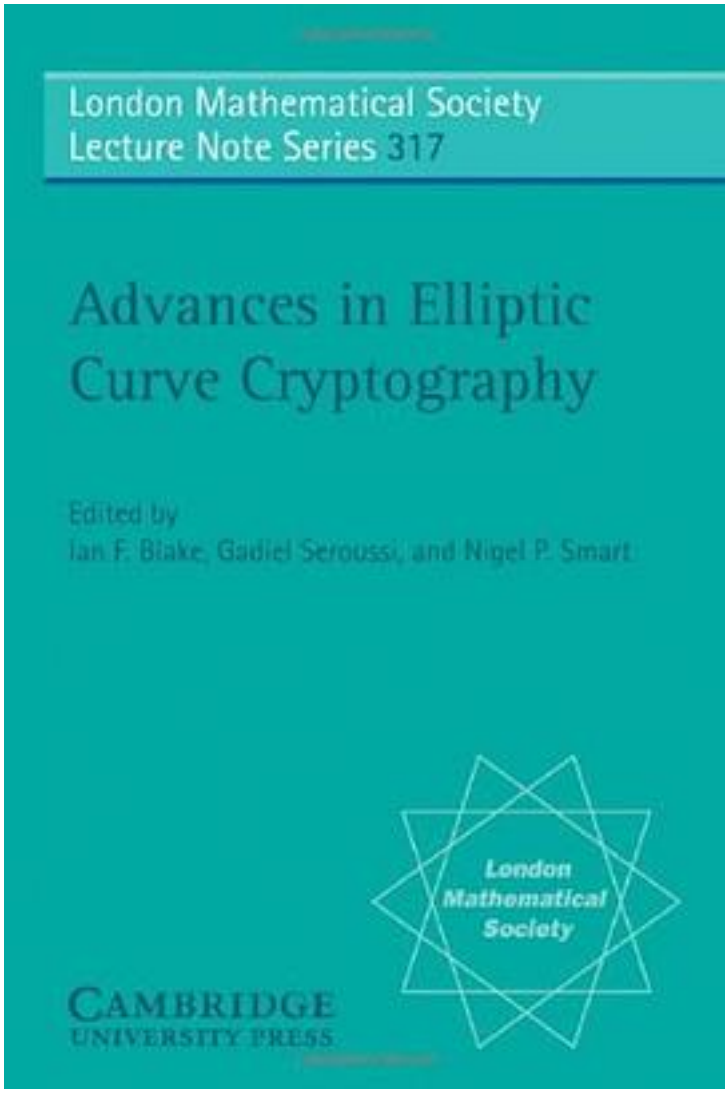
# Advances in Elliptic Curve Cryptography




Advances in Elliptic Curve Cryptography_下载链接1_

著者:Blake, Ian F. (EDT)/ Seroussi, Gadiel (EDT)/ Smart, Nigel P. (EDT)

出版者:Cambridge University Press

出版时间:2005-4-25

装帧:Paperback

isbn:9780521604154

Since 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.

作者介绍:

目录:

Advances in Elliptic Curve Cryptography_下载链接1_

## 标签

密码学

cryptography

## 评论

---
Advances in Elliptic Curve Cryptography_下载链接1_

## 书评

---
Advances in Elliptic Curve Cryptography_下载链接1_