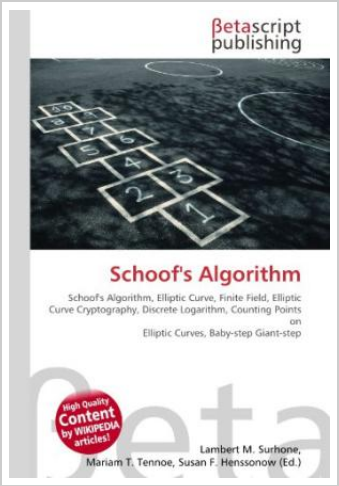

DOWNLOAD

Schoof's Algorithm

By Lambert M. Surhone

Betascript Publishers Jan 2010, 2010. Taschenbuch. Book Condition: Neu. 220x150x5 mm. Neuware - High Quality Content by WIKIPEDIA articles! Schoof's Algorithm is an efficient algorithm to count points on elliptic curves over finite fields. The algorithm has applications in elliptic curve cryptography where it is important to know the number of points to judge the difficulty of solving the discrete logarithm problem in the group of points on an elliptic curve. The algorithm was published by René Schoof in 1985 and it was a theoretical breakthrough, as it was the first deterministic polynomial time algorithm for counting points on elliptic curves. Before Schoof's algorithm, approaches to counting points on elliptic curves such as the naive and baby-step giant-step algorithms were, for the most part, tedious and had an exponential running time. This article explains Schoof's approach, laying emphasis on the mathematical ideas underlying the structure of the algorithm. 80 pp. Englisch.

READ ONLINE
[7.06 MB]

Reviews

It in a of the best ebook. It is one of the most incredible pdf i actually have go through. I am just easily will get a satisfaction of looking at a composed book.
-- ***Elisha McCullough***

I just started reading this article ebook. It really is writter in easy phrases and not difficult to understand. I am just very happy to tell you that here is the very best pdf we have read during my individual life and might be he very best ebook for actually.
-- ***Camren Kuvalis***