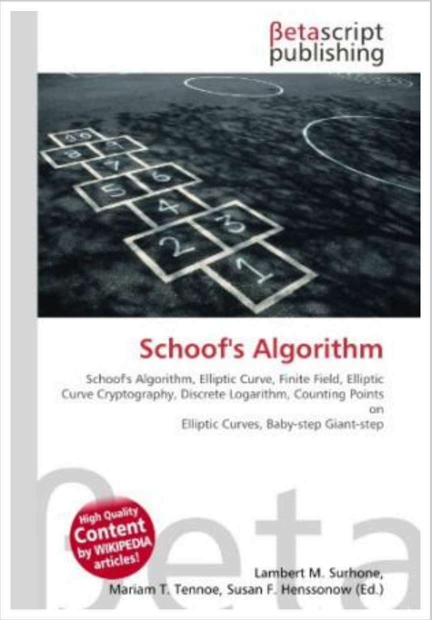
Betascript publishing
Schoof's Algorithm
Schoof's Algorithm, Elliptic Curve, Finite Field, Elliptic Curve Cryptography, Discrete Logarithm, Counting Points on Elliptic Curves, Baby-step Giant-step
High Quality Content by WIKIPEDIA articles!
Lambert M. Surhone, Mariam T. Tennoe, Susan F. Henssonow (Ed.)

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.

Reviews

This book may be really worth a read through, and far better than other. it was actually writtern extremely completely and valuable. I am just very easily will get a satisfaction of looking at a published ebook.

*-- **Lillie Toy***

It is easy in read through easier to fully grasp. it had been writtern very completely and useful. I am pleased to let you know that here is the greatest book we have read during my personal life and could be he very best book for possibly.

*-- **Miss Marge Jerde***