Computing Discrete Logarithms in an Interval

http://www.firstlight.cn 2010-12-01

The discrete logarithm problem in an interval of size N in a group G is: Given $g, h \in G$ and an integer $ N$ to find an intege r $0 \le n \le N$, if it exists, such that $h = g^n$. Previously the best low-storage algorithm to solve this problem was the van Oorschot an d Wiener version of the Pollard kangaroo method. The heuristic average case running time of this method is $(2 + o(1)) \sqrt{N}$ group ope rations.

We present two new low-storage algorithms for the discrete logarithm problem in an interval of size N. The first algorithm is based o n the Pollard kangaroo method, but uses 4 kangaroos instead of the usual two. We explain why this algorithm has heuristic average case exp ected running time of $(1.714 + o(1)) \sqrt{N}$ group operations. The second algorithm is based on the Gaudry-Schost algorithm and the id eas of our first algorithm. We explain why this algorithm has heuristic average case expected running time of $(1.660 + o(1)) \sqrt{N}$ gro up operations. We give experimental results that show that the methods do work close to that predicted by the theoretical analysis.

存档文本