CORR 99-07

Some baby-step giant-step algorithms for the low hamming weight discrete logarithm problem

D.R. Stinson

Abstract We present several baby-step giant-step algorithms for the low hamming weight discrete logarithm problem. In this version of the discrete log problem, we are required to find a discrete logarithm in a finite group, given that the unknown logarithm has a specified number of 1's in its binary representation. Heiman and Odlyzko presented the first algorithms for this problem. Unpublished improvements by Coppersmith include a deterministic algorithm with complexity $O\left(m\binom{\frac{m}{2}}{\frac{t}{2}}\right)$, and a Las Vegas algorithm with complexity $O\left(\sqrt{t}\binom{\frac{m}{2}}{\frac{t}{2}}\right)$.

We perform an average-case analysis of Coppersmith's deterministic algorithm. The average-case complexity achieves only a constant factor speed-up over the worst-case. Therefore, we present a generalized version of Coppersmith's algorithm, utilizing a combinatorial set system that we call a *splitting system*. Using probabilistic methods, we prove a new existence result for these systems that yields a deterministic algorithm with complexity $O\left(t^{3/2}(\log m)\binom{\frac{m}{2}}{\frac{t}{2}}\right)$. We also present some explicit constructions for splitting systems that make use of perfect hash families.