

The Discrete Logarithm Problem and Ternary Functional Graphs

Max F. Brugger Christina A. Frederick

September 8, 2007

Abstract

Encryption is essential to the security of transactions and communications, but the algorithms on which they rely might not be as secure as we all assume. In this paper, we investigate the randomness of the discrete exponentiation function used frequently in encryption. We show how we used exponential generating functions to gain theoretical data for mapping statistics in ternary functional graphs. Then, we compare mapping statistics of discrete exponentiation functional graphs, for a range of primes, with mapping statistics of the respective ternary functional graphs.