

The Discrete Logarithm Hides $O(\log n)$ Bits

Douglas Long
Avi Wigderson

Abstract

The main result of this paper is that obtaining any information about the $O(\log |p|)$ “most significant” bits of x , given $g^x \pmod{p}$, even with a tiny advantage over guessing, is equivalent to computing discrete logarithms \pmod{p} .