Vol. 88, No. 2 DUKE MATHEMATICAL JOURNAL © 1997

ZETA FUNCTIONS, ONE-WAY FUNCTIONS, AND PSEUDORANDOM NUMBER GENERATORS

MICHAEL ANSHEL AND DORIAN GOLDFELD

§1. Introduction. A central problem in cryptography is to establish the existence of one-way functions. Such a function would have the property that, while it is computable in polynomial time, its inverse is not. One approach to this problem is to construct candidate one-way functions from seemingly intractable problems in number theory. We introduce a new intractable problem arising from the theory of zeta functions which leads to a new class of one-way functions based on the arithmetic theory of zeta functions. Moreover, there appears to be no relation between this problem and other intractable problems, such as integer factorization and the computation of discrete logarithms, where known attacks have emerged in recent years (see [22] and [26]). At present, the authors are unaware of any methods at all that would provide an attack on our candidate one-way functions.

It is a consequence of the main theorem of [12] that a one-to-one one-way function implies the existence of a pseudorandom number generator. The construction of such pseudorandom number generators, however, is computationally intensive. In our case we explicitly construct from a given elliptic curve a pseudorandom number generator $\mathrm{PNG}_{\mathrm{Elliptic}}$, which can be computed very efficiently and at low computational cost. Under the assumption that two different classes of zeta functions (the elliptic class and the Artin class, to be defined below) give rise to one-way functions, we prove that an elliptic curve satisfying certain hypotheses implies the existence of such a pseudorandom number generator. In this regard, the second author would like to take this opportunity to thank Fred Diamond for many helpful discussions concerning ℓ-adic representations.

§2. One-way functions and the feasible Selberg class. Let $n \geqslant 0$ be an integer, and define

$$d_2(n) = \begin{cases} \lfloor \log_2 n \rfloor + 1, & \text{if } n > 0 \\ 1, & \text{if } n = 0, \end{cases}$$

where for an arbitrary real number $x \geqslant 0$, $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x. We refer to $d_2(n)$ as the bit size of n. We extend this notion to nonnegative integral vectors by defining the norm $||(n_1, n_2, \ldots, n_t)||$ of a vector

Received 25 June 1996. Revision received 10 July 1996.