ON THE BIT-SECURITY OF RSA

JOHAN HÅSTAD

The RSA encryption function is widely believed to be a one-way function. By a one-way function we mean a function that is easy (polynomial time) to compute and hard (not polynomial time) to invert.

Being a one-way function does not rule out the possibility that each individual bit of the input can be guessed efficiently with a good probability, (say 3/4) of being correct. If such a guessing procedure existed extreme care would be needed when using RSA for cryptography.

Using the multiplicativity of the RSA function, however, it is possible to prove that it has properties that are not shared by general oneway functions. It was proved already in 1984 by Alexi, Chor, Goldreich and Schnorr that, provided that the RSA function is one-way, the least significant bit of the input cannot be guessed with any significant advantage over a random guess.

These results were later extended by Håstad and Näslund to cover each individual bit of the input.

We will outline the methods used to obtain these results and, to some extent, discuss extensions to other problems.

Royal Institute of Technology