The cost of integer factorization

D. J. Bernstein
University of Illinois at Chicago

NSF DMS–0140542

`http://cr.yp.to`
`/nfscircuit.html`

Number of key bits needed to protect against NFS:

attacker uses			need B/X bits
sieving	matrix	min	where X is
RAM	RAM	ops	$3.375 + o(1)$
RAM	RAM	cost	$3.057\ldots + o(1)$
circuit	RAM	cost	$1.308\ldots + o(1)$
circuit	circuit	cost	$1.121\ldots + o(1)$

This is the easy part of the analysis.

What about 1024, 1536, 2048?

Myth: $o(1)$ is 0. **Fact:** $o(1)$ says nothing about specific key sizes.

Myth: My sample circuit is the best circuit. **Fact:** Need to analyze many different circuits.

This is the hard part of the analysis.