The NSA sieving circuit

D. J. Bernstein
University of Illinois at Chicago

NSF DMS–9970409

Cost to sieve y^2 polynomial values using primes $\leq y$:

Method	Hardware	Time
Cracker	$y^{1+o(1)}$	$y^{2+o(1)}$
TWINKLE	$y^{1+o(1)}$	$y^{2+o(1)}$
RAM sieving	$y^{1+o(1)}$	$y^{2+o(1)}$
NSA circuit	$y^{1+o(1)}$	$y^{3/2+o(1)}$
3-D version	$y^{1+o(1)}$	$y^{4/3+o(1)}$

Method to sieve y values:
Generate $y^{1+o(1)}$ pairs (q, v).
Sort in order of v.

RAM sieving: distribution sort.

NSA circuit: mesh sort.