Non-Wafer-Scale Sieving Hardware for the NFS: Another Attempt to Cope with 1024-bit

Willi Geiselmann
Rainer Steinwandt

The Number Field Sieve

- Precomputation
- Relation collection
- Linear Algebra (Matrix step)
- Postprocessing

Relation Collection

- Given $F_1(x,y)$, $F_2(x,y) \in \mathbb{Z}[x,y]$, *homogeneous polynomials, e.g. of degree 5 and 1*
- Find $(a,b) \in \mathbb{Z} \times \mathbb{N}$ with $F_1(a,b)$ and $F_2(a,b)$ smooth, $\gcd(a,b) = 1$

Parameters for 1024 Bit (identical with TWIRL, 2003)

- Smoothness bounds:

  $B_1 = 2.6 \cdot 10^{10}$ (algebraic),

  $B_2 = 3.5 \cdot 10^{9}$ (rational).

- Sieving region:

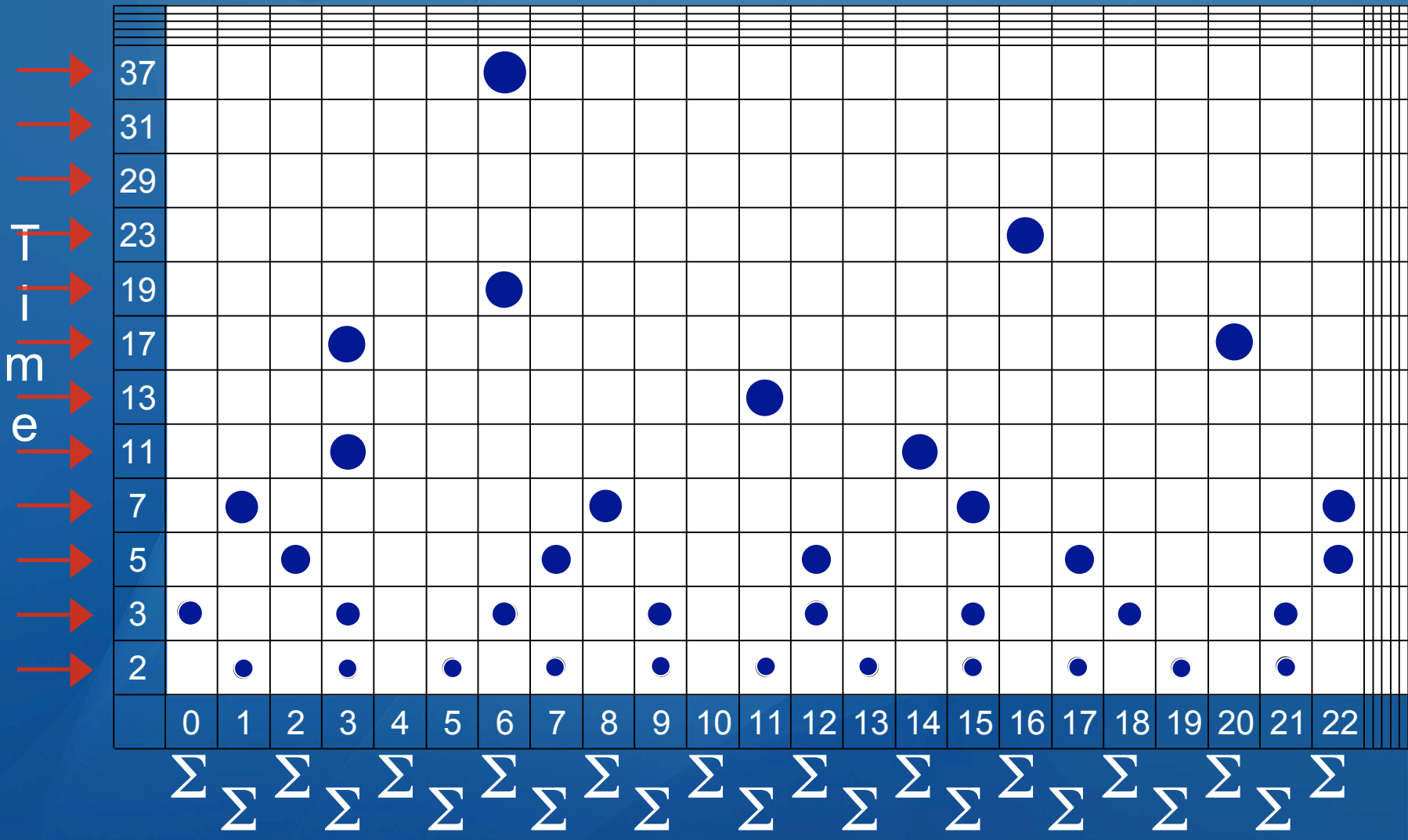
  $A = 5.5 \cdot 10^{14}$, $-A < a < A$;

  $B = 2.7 \cdot 10^{8}$, $0 < b < B$.

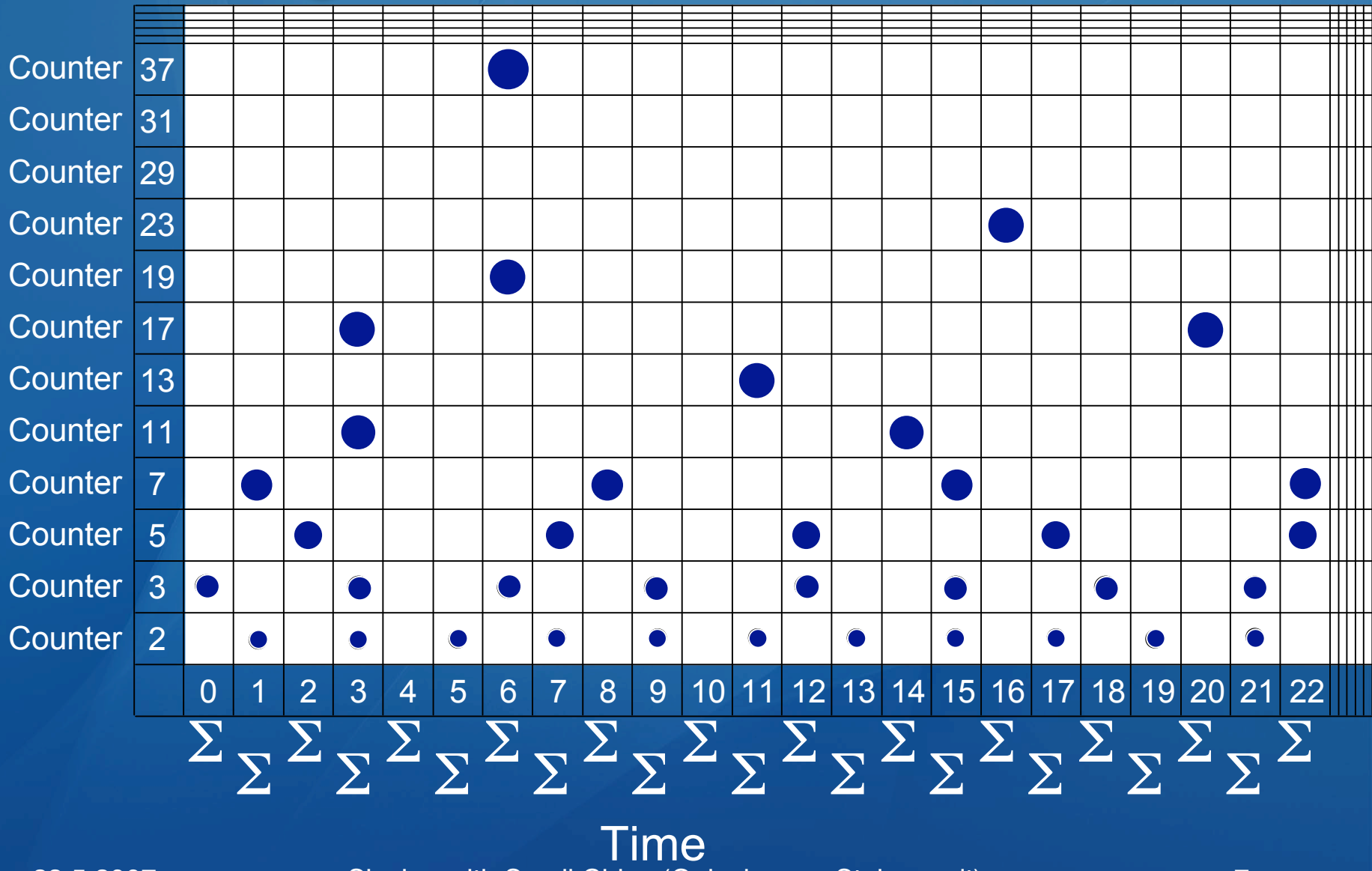
Previous work

- TWINKLE [Shamir 1999; Shamir, Lenstra 2000]
  not designed for 1024 bit numbers
- TWIRL [Shamir, Tromer 2003]
  full wafer design
- Mesh-based sieving [G., St. 2003, 2004]
  not feasible for 1024 bit numbers
- SHARK [Franke et al. 2005]
  elaborated butterfly transport system

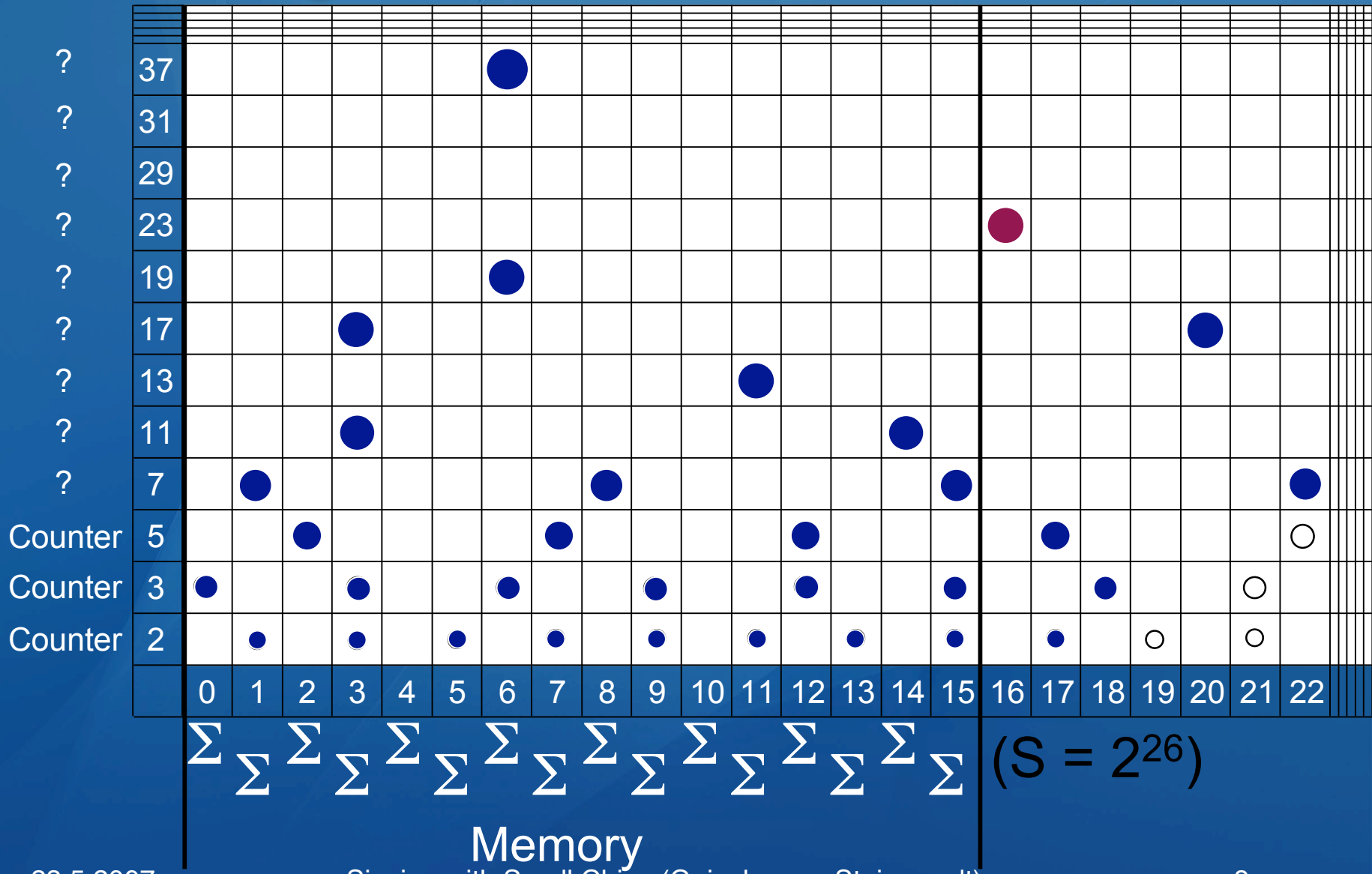
Sieving (Eratosthenes)



Sieving (TWINKLE/TWIRL)



Sieving (mesh / here)

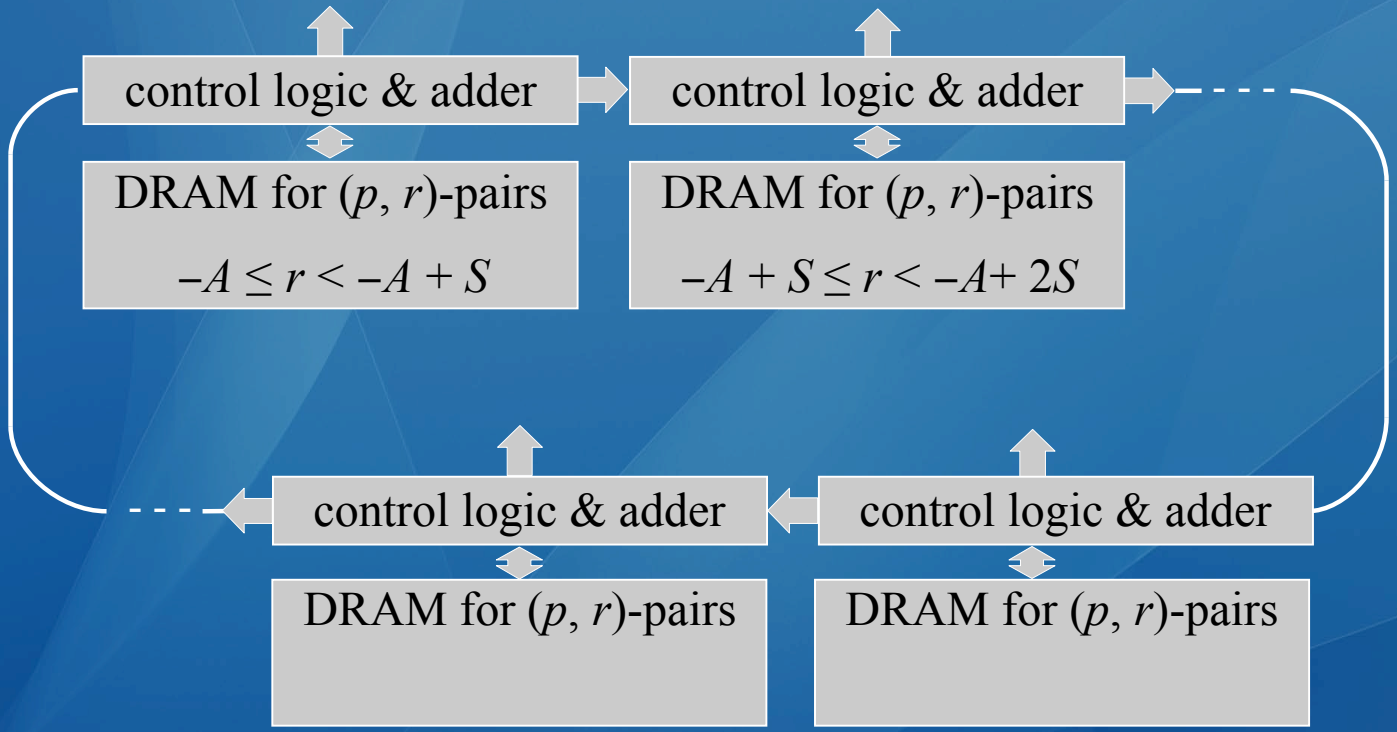


Different Types of Primes

- Largish primes I: $2^{27.2} < p < B_1 < 2^{35}$

  ...Type II/III: $1.5 \cdot 10^7 < p < 2^{27.2}$
- Medium primes: $2^{13} < p < 1.5 \cdot 10^7$
- Smallish primes: $p < 2^{13}$

Largish Stations

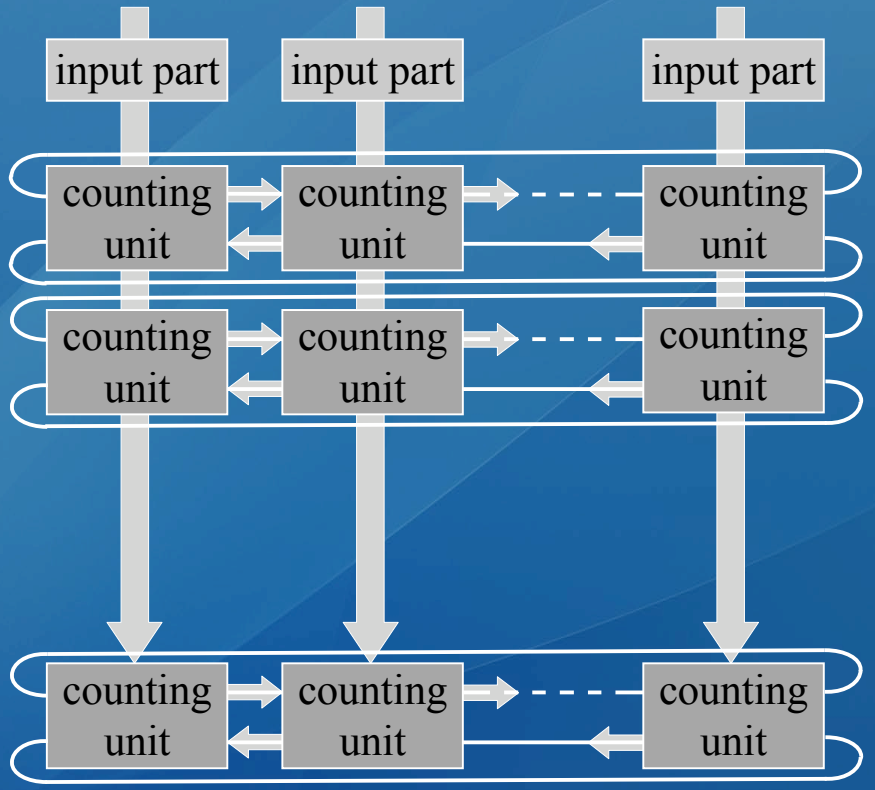


Largish Stations (Type I)

- DRAM holds < 100,000 (p,r)-pairs
- 3 < #DRAMs < 389 (p_{max} / S)
- 256 stations for $p > 1.5 \cdot 10^7 \approx 2^{27.2}$
- Distributed on 32 chips:
  size: 472 mm^2 (0.13 µm process)
  output: 448 bit per clock cycle
  memory: 99%, logic: 1%

Collection Unit

- Distributed on 4 chips, each holding
- 4 arrays of 32 x 32 counting units.
- Each unit is in charge of 2^{12} sieve locations,
- and adding up the log(p) values.



Medium and Smallish Primes

- Medium Primes:
  - Calculated close to the Counting Units
- Smallish Primes:
  - calculated in the Counting Parts
  - stored (added) in separate DRAM

Collection Unit (area estimates)

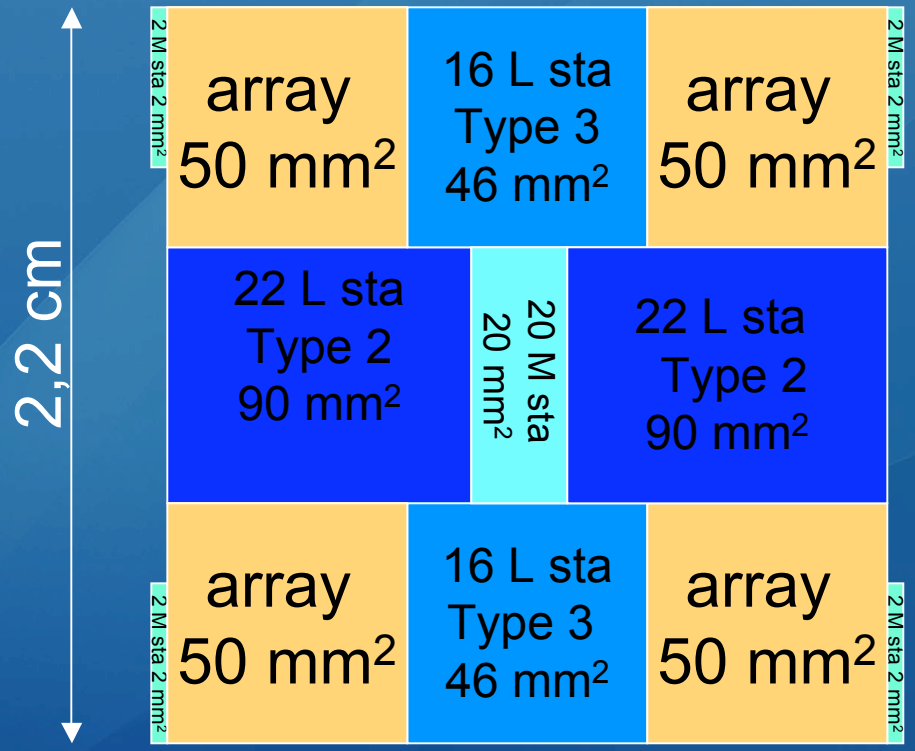
Distributed on 4 chips:

size: 493 mm²
(0.13 μm process)

input: 3584 bit / cc

memory: 94%

logic: 6%



Performance

- Total silicon area 172 cm^2
- One subinterval ($S=2^{26}$) in 53,000 cc
- One sieve line in 25 min (600 MHz)
- Sieving of a 1024 bit number with 8300 devices in one year
- 3.5 x more silicon area than TWIRL
- or 2.0 x more after modification