SHARK

A Realizable Special Hardware Sieving Device for Factoring 1024-bit Integers

Jens Franke, Thorsten Kleinjung - University of Bonn

Christof Paar, Jan Pelzl - University of Bochum

Christine Priplata, Colin Stahlke - EDIZONE GmbH, Bonn

Outline

- Why SHARK - Factoring 1024-bit Integers?
- General Number Field Sieve and Lattice Sieving
- Hardware Sieving Devices
- SHARK Sieving Device - Architecture
- Butterfly Transport System
- Cost Estimates
- Concluding Remarks

RSA and Factoring

To break RSA it suffices to factor the used modulus N.

$N=pq$	p, q extremely large primes

Best knowledge of today:

Apparently breaking RSA is as hard as factoring N.

Integer Factorization

Up to now no polynomial time algorithm is known.

The **G**eneral **N**umber **F**ield **S**ieve (GNFS) is currently the best method available to attack RSA by trying to factor N.

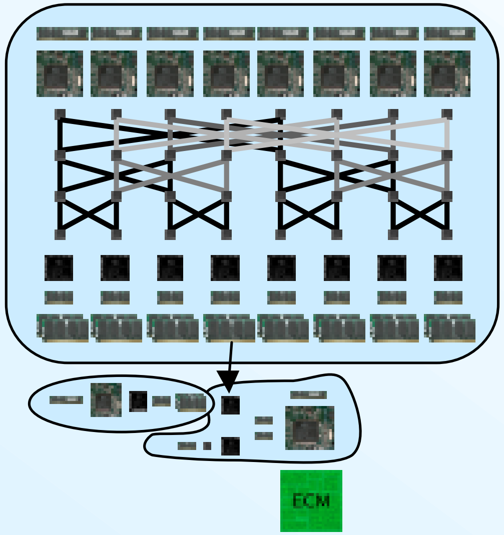
The expensive steps of GNFS:

- sieving step: find enough pairs $(a,b) \in \mathbb{Z}^2$
- matrix step: next talk

RSA with 663 bit has been broken in software.

Why SHARK?

Cracking RSA-1024

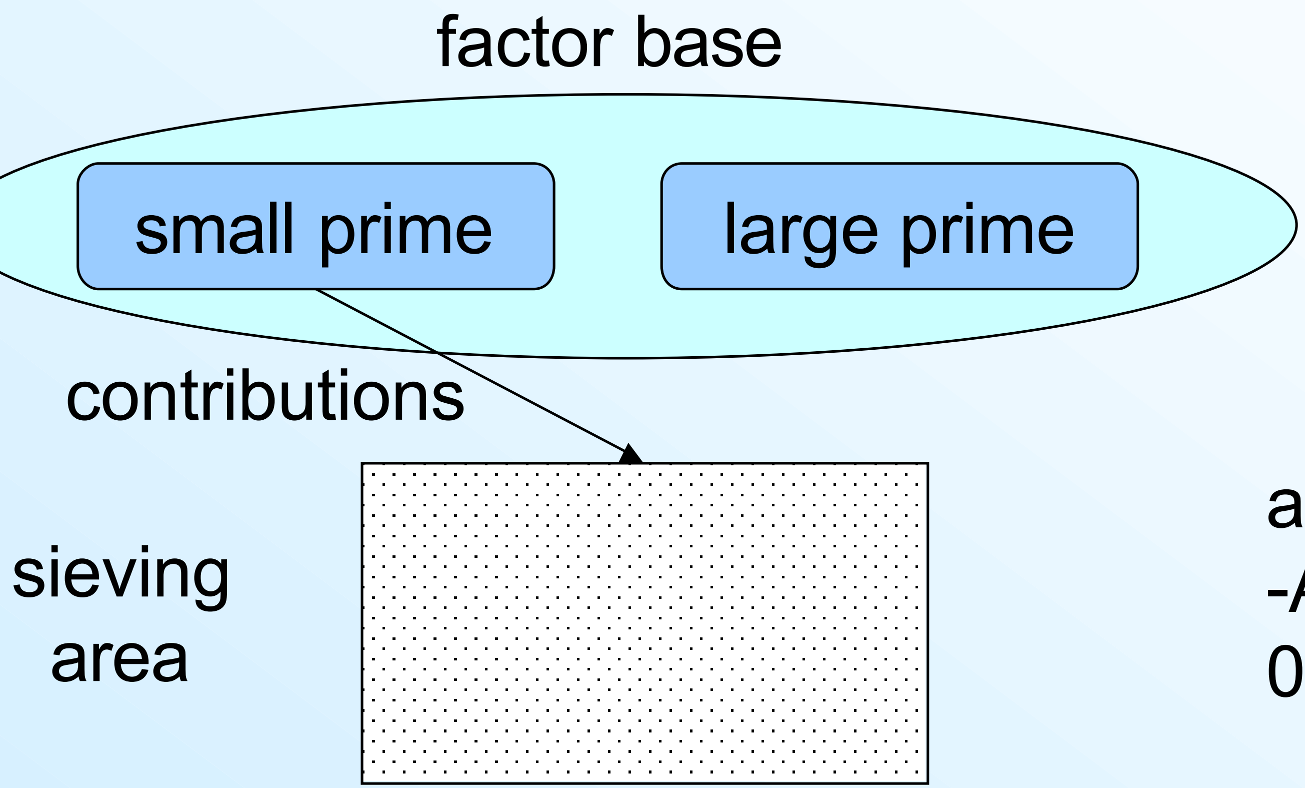


Can we do it with today´s conventional technology

for less than 1 000 000 000 US dollars?

General Number Field Sieve, Sieving Step

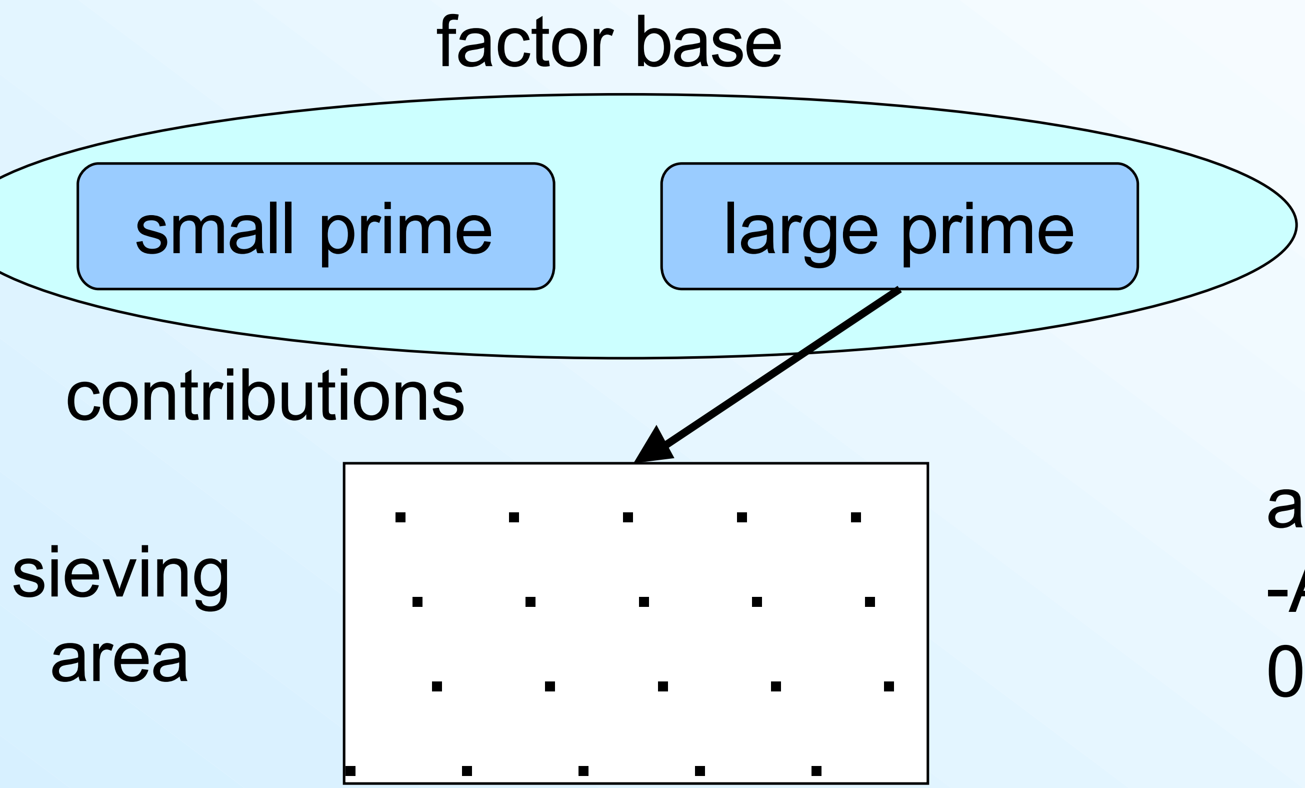
For each prime p of the factor base add contribution log(p) to certain locations in the sieving area.



$a,b \in \mathbb{Z}^2$
$-A<a<A$
$0<b<B$

General **N**umber **F**ield **S**ieve, Sieving Step

For each prime p of the factor base add contribution log(p) to certain locations in the sieving area.



$a,b \in \mathbb{Z}^2$

$-A<a<A$

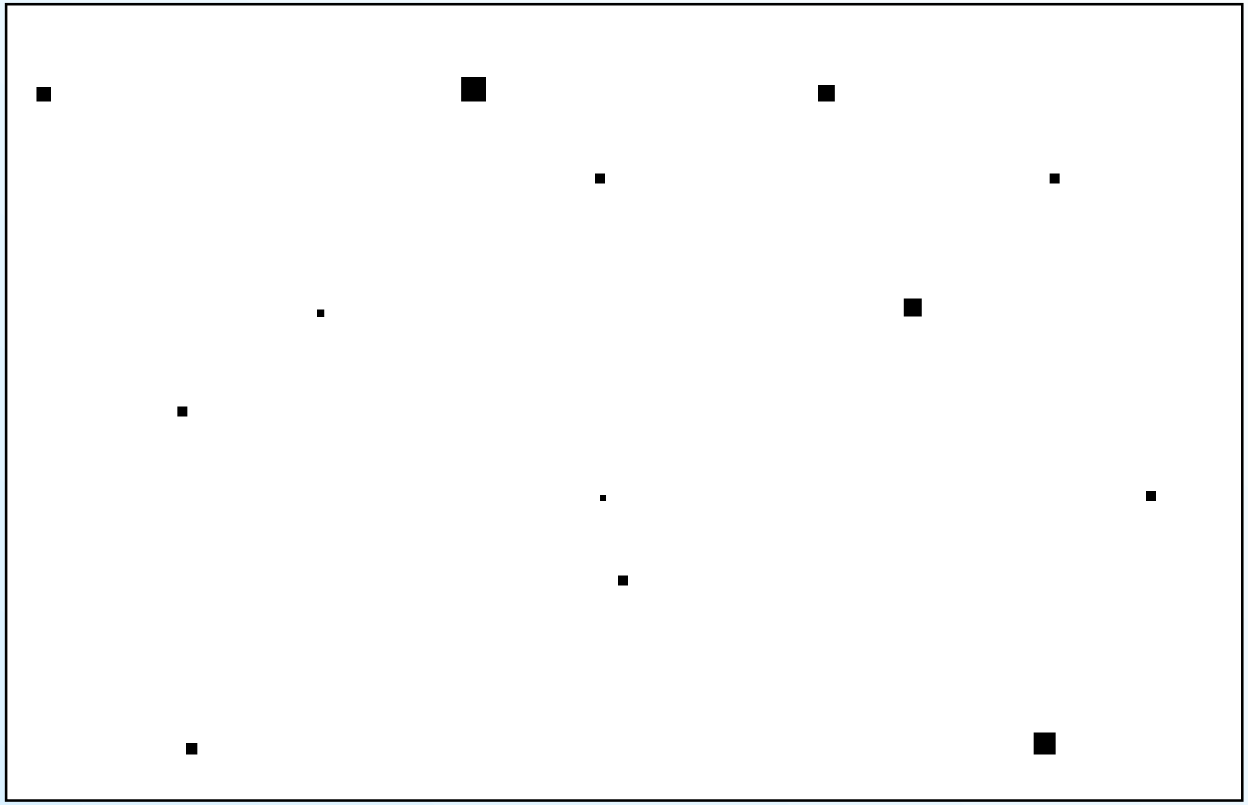
$0<b<B$

General Number Field Sieve

Summing up contributions yields:

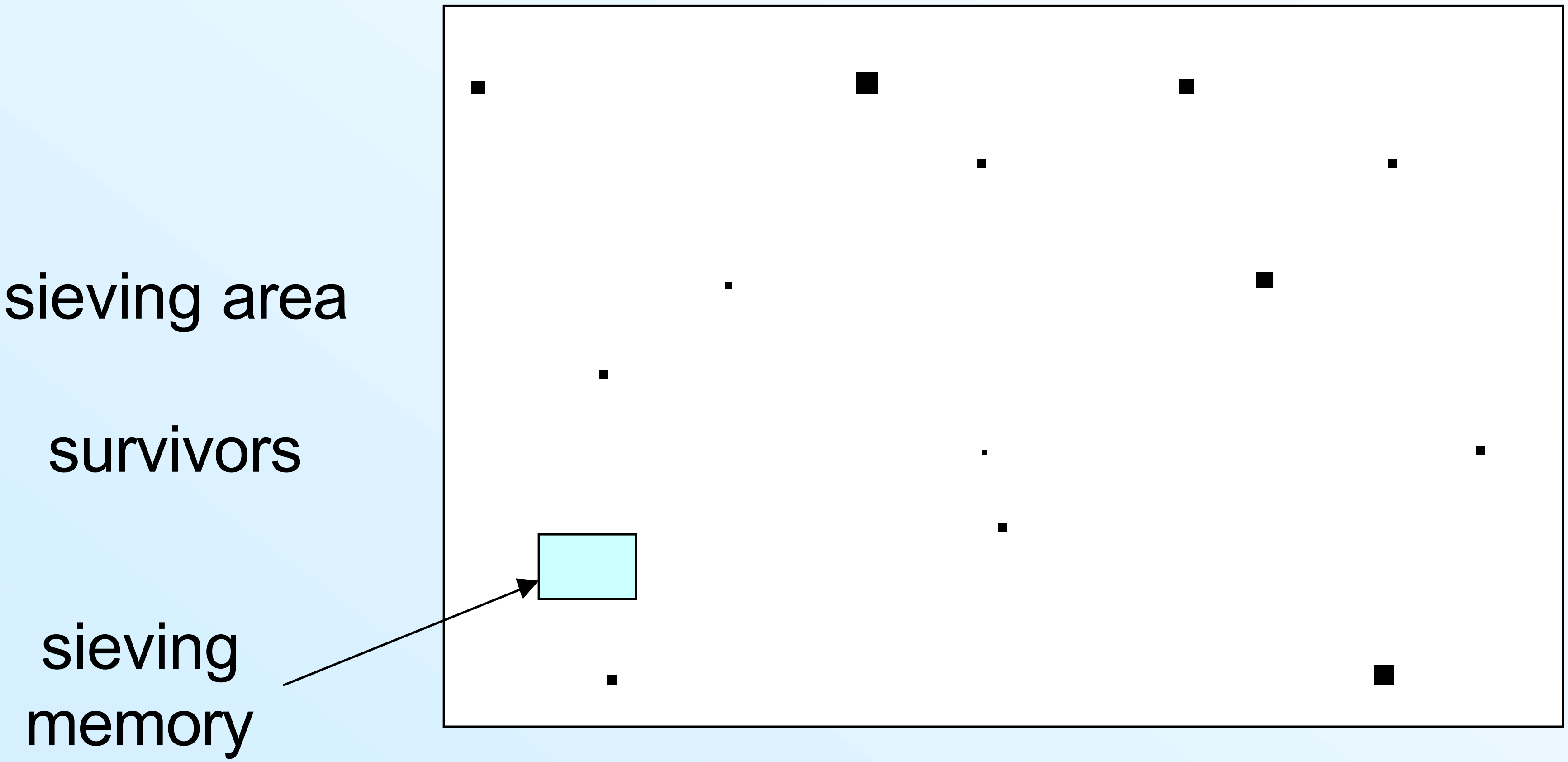
sieving area

survivors



General Number Field Sieve

Summing up contributions yields:



Sieving Procedure

- Create contribution data (p, log p, e)
  - p: factor base element
  - log p: size of contribution
  - e: position of contribution

- “Sort“ contribution data w.r.t. position e

- For each position e in the sieving area check if

$$\sum_{(p,\log p,e)} \log p \quad > \quad \text{bound depending on } e$$

Lattice Sieving

Only consider most promising candidates (a,b)

(i.e. choose large primes q, for each q consider those (a,b) where q is contributing to)

Advantage:
- more survivors (i.e. needs less sieving)

Drawbacks:
- complexer computations
- higher initialization costs
- duplicates

Lattice sieving is the most efficient sieving technique.

And now for something completely different

Sieving Step of GNFS in Hardware

A short history of hardware sieving devices:

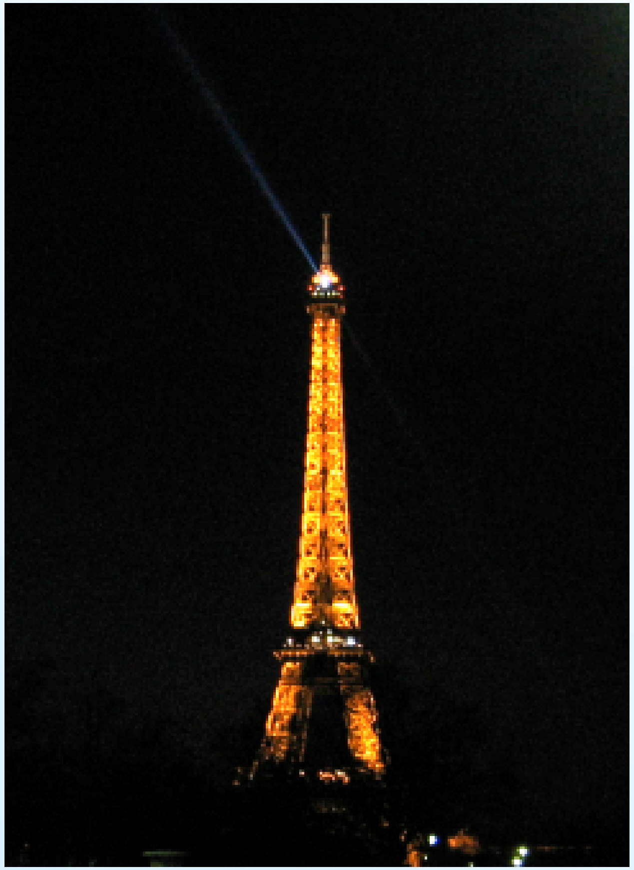
- 1999: TWINKLE
- 2003: TWIRL
- 2004: YASD
- 2005: SHARK

Supporting GNFS with cofactorization:

- ECM implementation on FPGA (SHARCS 2005)

TWINKLE

TWINKLE by A. Shamir, optical device for 512 to 768 bit (CHES 1999)



TWIRL

TWIRL by A. Shamir and E. Tromer, pipelined architecture for 1024 bit RSA (Crypto 2003)

Yet **A**nother **S**ieving **D**evice

YASD by W. Geiselmann and R. Steinwandt, mesh sorting device for 1024 bit RSA, adapts ideas of D. Bernstein (CT-RSA 2004)

SHARK

SHARK by J. Franke, T. Kleinjung, C. Paar, J. Pelzl, C. Priplata, C. Stahlke for 1024 bit RSA (SHARCS 2005)

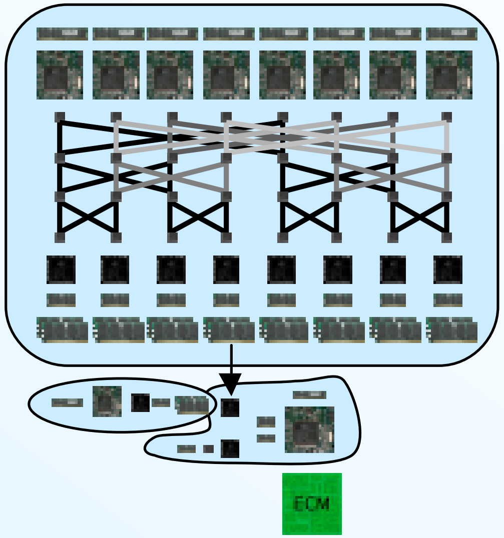
SHARK - switched on

SHARK by J. Franke, T. Kleinjung, C. Paar, J. Pelzl, C. Priplata, C. Stahlke for 1024 bit RSA (SHARCS 2005)

SHARK

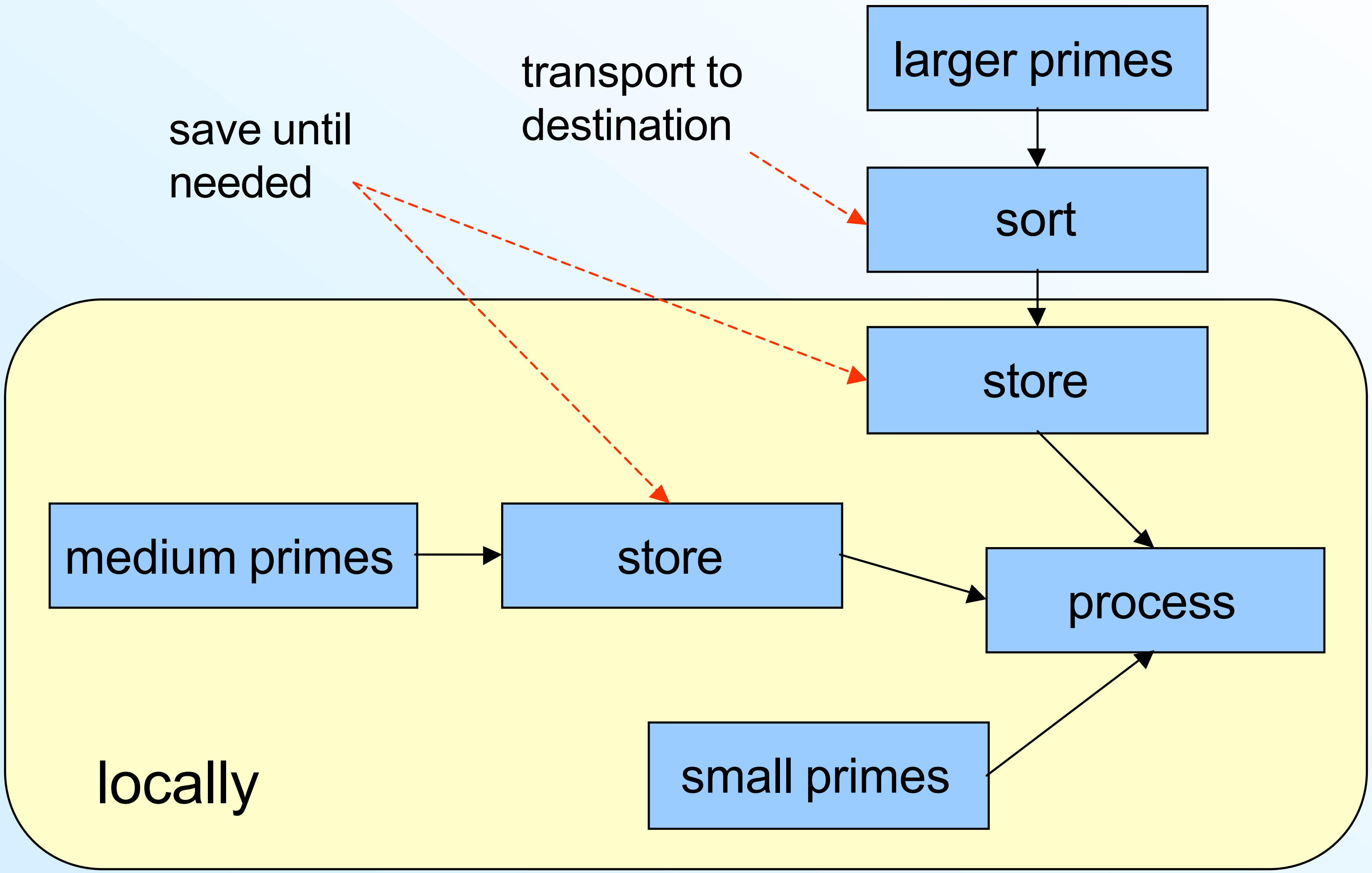
SHARK uses lattice sieving to perform the sieving step of GNFS for a 1024-bit integer within a year for around 200 million US dollars.

- 2300 identical machines
- small specialized ASICs
- of-the-shelf RAM
- modular architecture
- conventional data buses

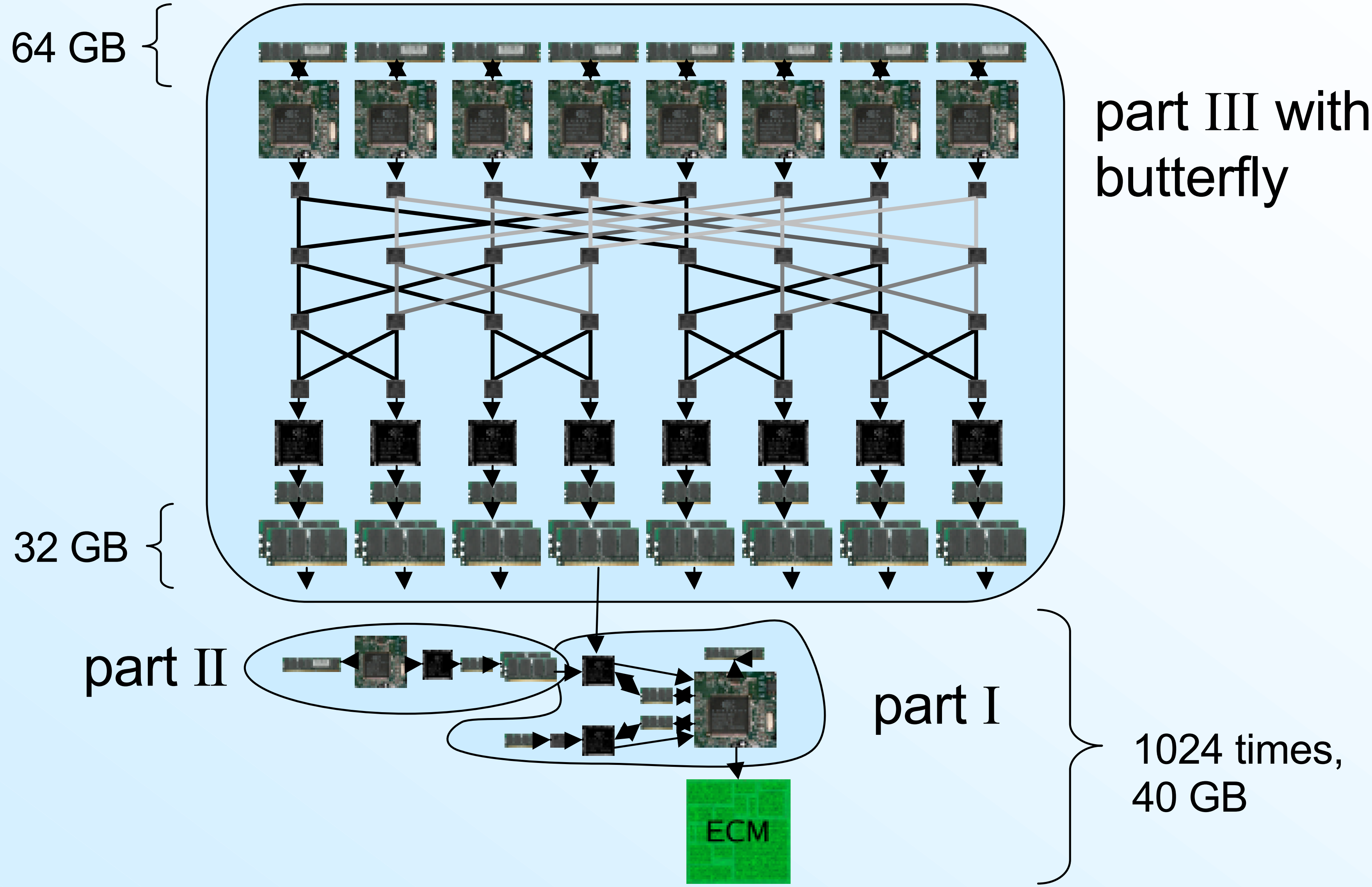


The price (without development costs) is an upper bound and can be lowered considerably by changing the parameters.

SHARK's Main Structure



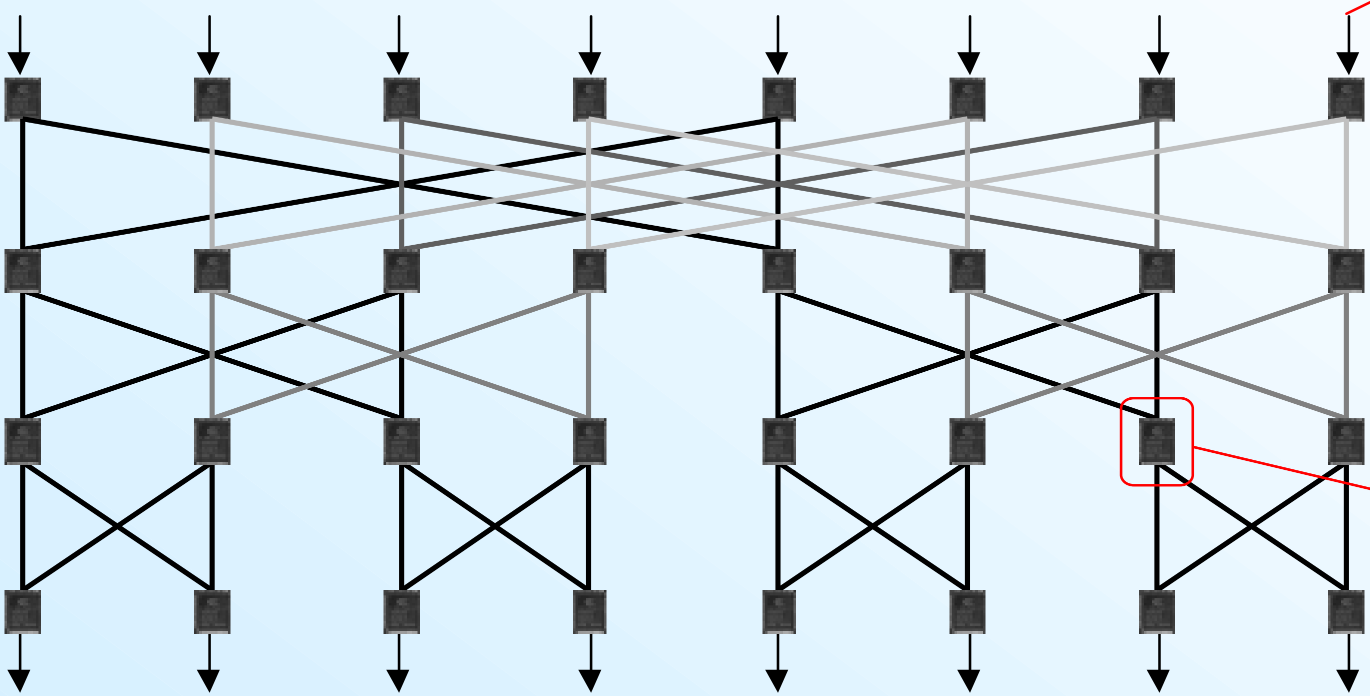
SHARK Architecture



Butterfly Transport System

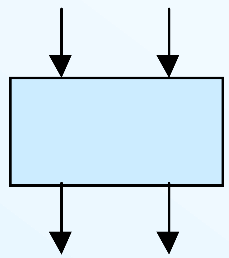
2^n input channels

peak : 1 GB/s
average: 0.2 GB/s



n+1 layers

2 inputs,
small
input buffers



2 outputs

2^n output channels

SHARK: n=10

Rough Cost Estimates

1 machine:

memory:	136 GB RAM + 192 MB cache	21 000 $
processors:	1/4 wafer + transport system	9 000 $
power supply + additional electronic + cooling:		30 000 $
PCs (control) + ECM (negligible):		10 000 $
		70 000 $
power consumption: 30 kW	per year	25 000 $

2300 machines complete the sieving step in one year and cost

160 million US $ + 60 million US $ electricity.

© EDIZONE GmbH, Uni Bochum, Uni Bonn

Concluding Remarks

SHARK can perform the sieving step for a 1024-bit integer factorization in 1 year and costs around 200 million US $ (pessimistic estimate).

- modular design, small ASICs, conventional memory chips
- possible improvements: better choice of parameters, more ECM, resize transport system
- realizable with today´s technology

Any questions?