An Evaluation of the Sieving Device YASD for 1024-bit Integers*

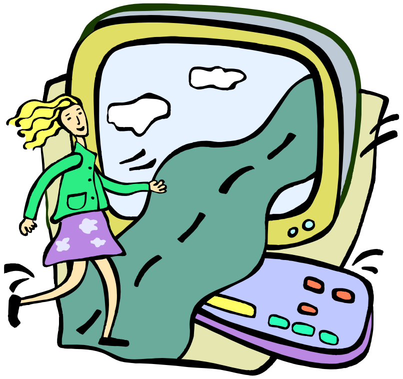
SHARCS 2006, Cologne, Germany
April 4, 2006

Naoyuki Hirota (UEC), ○**Tetsuya Izu (FUJITSU),**
Noboru Kunihiro (UEC), Kazuo Ohta (UEC)

* A part of this work is financially supported by a consignment research from the National Institute of Information and Communications Technology (NICT), Japan.

Integer Factoring in Security

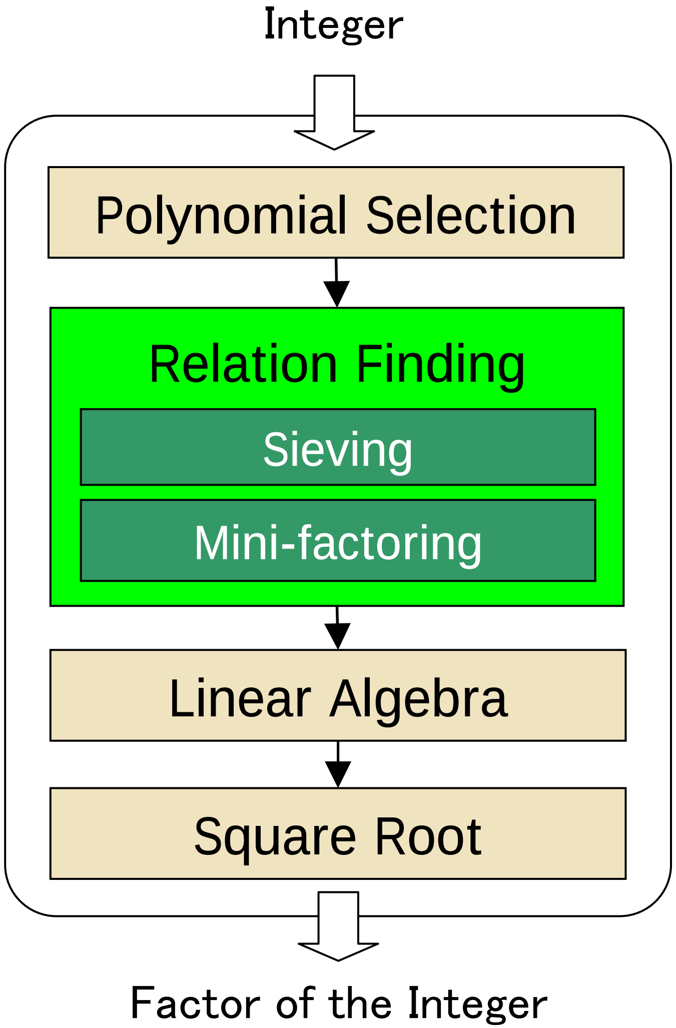
- Integer factoring is hard in theory and practice
  - This property assures the RSA's security
  - The best factoring algorithm: Number Field Sieve method (NFS)
    - World record: "RSA200", a 663-bit integer (May 2005)
    - Since NFS is sub-exponential time algorithm, factoring 1024-bit integer seems far away…
  - In some standards, it is strongly believed that factoring 1024-bit integers, RSA's default key size, will be infeasible at least in next 10 years



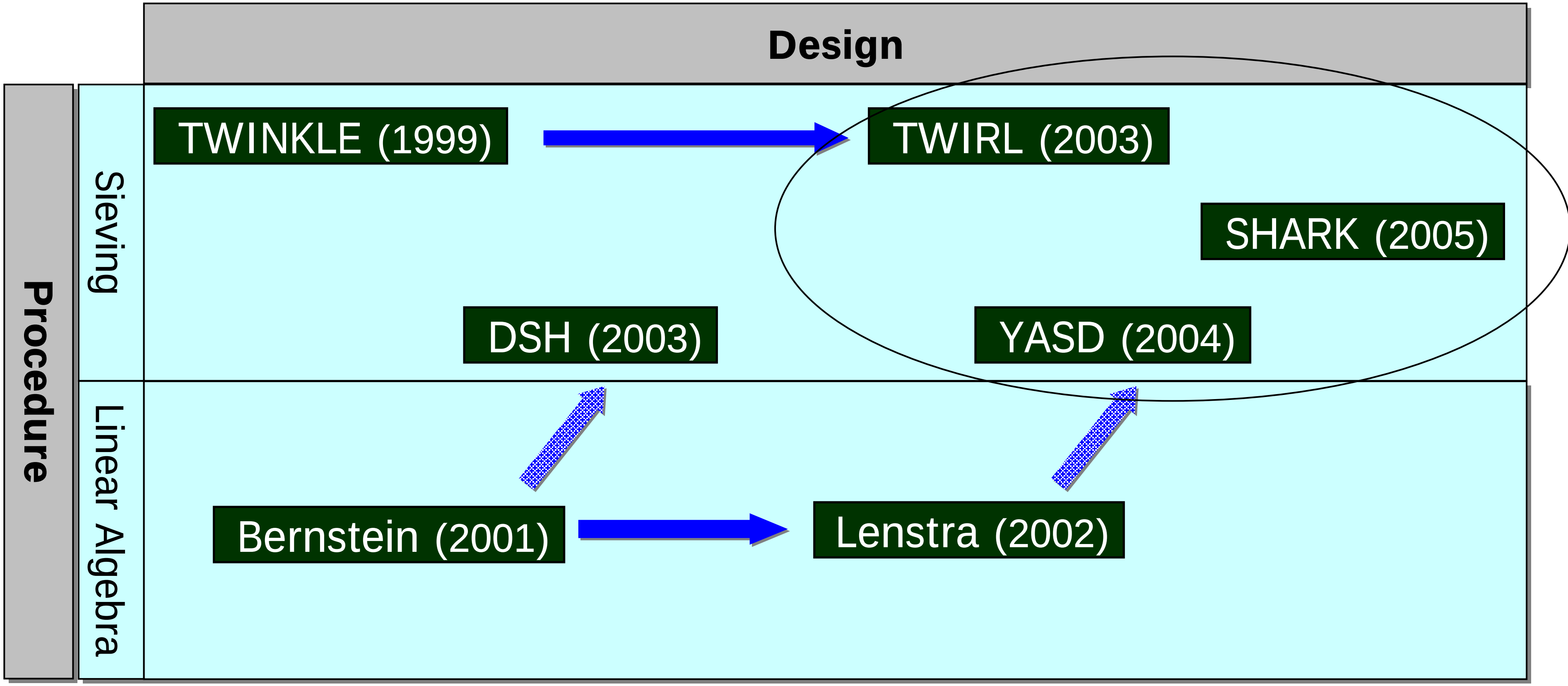
Number Field Sieve Method (NFS)

- 4 major steps in NFS
  - Polynomial Selection
  - Relation Finding
    - Sieving
    - Mini–factoring
  - Linear Algebra
  - Square Root

- Time-consuming Steps
  - Relation Finding
    - Sieving
  - Linear Algebra



Dedicated Factoring Hardware



Comparison

	1024-bit	768-bit
TWIRL	Size: $15960\text{mm}^2 \times 8 + 66000\text{mm}^2$ Time: 194 years (by 1 set) Cost: 15000 USD/set Frequency: 1 GHz	Size: $1330\text{mm}^2 + 4430\text{mm}^2$ Time: 2.3 years (by 1 set) Cost: 750 USD/set Frequency: 1 GHz
YASD	**Size: 42200mm^2** **Time: 10301 years (by 1 set)** **Cost: 3200 USD/set** **Frequency: 500 MHz**	Size: 2400mm^2 Time: 34.5 years (by 1 set) Cost: 250 USD/set Frequency: 500 MHz
SHARK	Size: ¼wafer+DRAM Time: 2300 years (by 1 set) Cost: 40000 USD/set Frequency: 1 GHz	

Rough Estimation !
Especially, we did not consider wiring problem and mini-factoring problem…

Assumed 130 nm technology, full wafers with 300 mm diameter.
Cost estimation excludes NRE, defects and power supply.

Contents

- Introduction
- Description of YASD
- Time Parameterization
- Area Parameterization
- Formulas and Optimization
    - Generalized YASD
    - YASD for 768-bit Integers (YASD768)
    - YASD for 1024-bit Integers (YASD1024)
- Concluding Remarks

Contents

- Introduction
- Description of YASD
- Time Parameterization
- Area Parameterization
- Formulas and Optimizations
  - Generalized YASD
  - YASD for 768-bit Integers (YASD768)
  - YASD for 1024-bit Integers (YASD1024)
- Concluding Remarks

YASD (Yet Another Sieving Device)

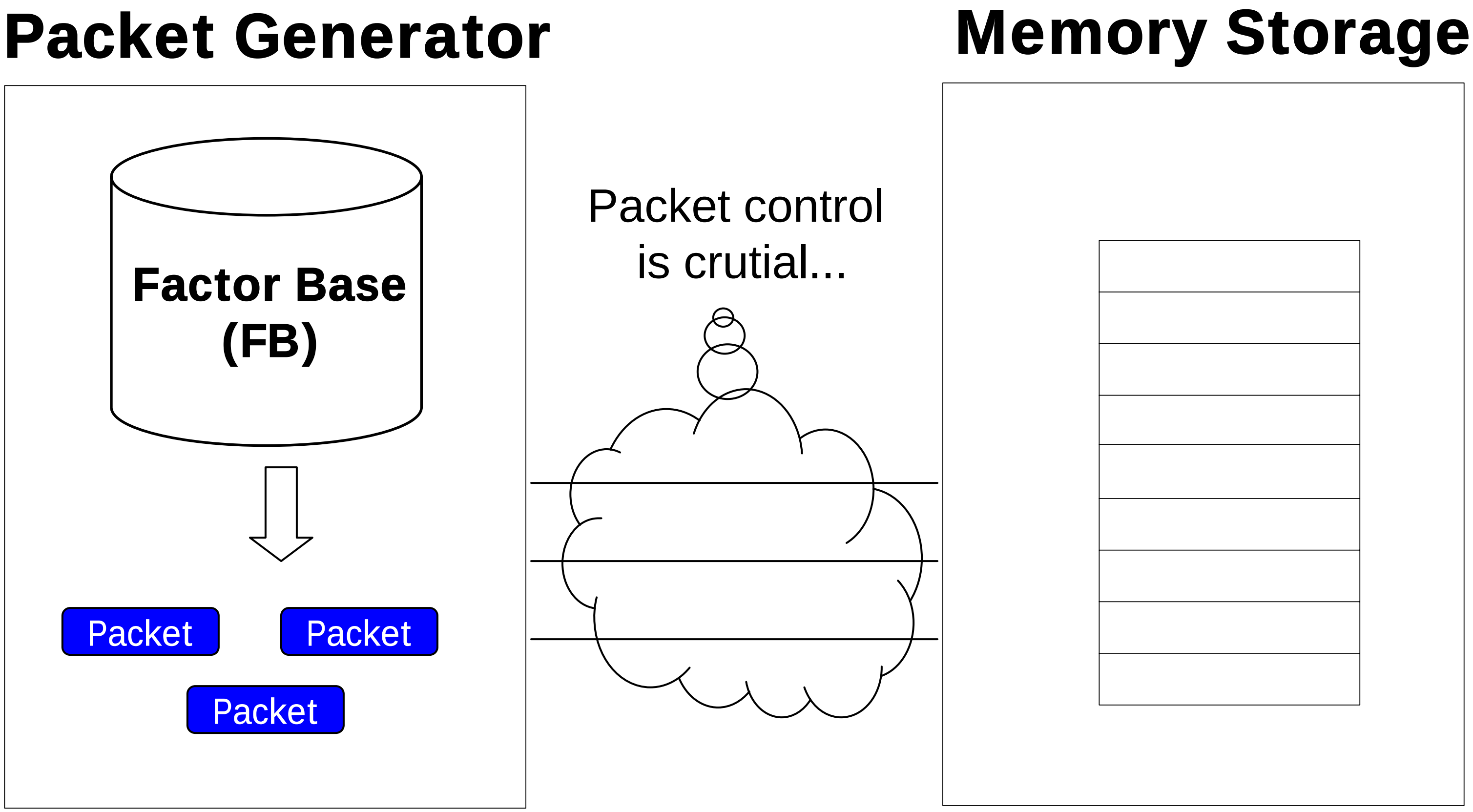
- Dedicated Sieving Device
  - Proposed by Willi Geiselmann and Rainer Steinwandt in CT-RSA 2004
  - No implementational results have been reported

- Idea : Use of the Clockwise Routing Algorithm
  - A mesh of processing nodes
  - Regular structure
  - Assumed 130 nm technology, wafer with 300 mm diameter and 500 MHz frequency
  - 768-bit integer can be sieved in 600 days with 21 YASDs (here manufacturing cost is assumed to be 5000 USD)

What Does the Sieving Do?

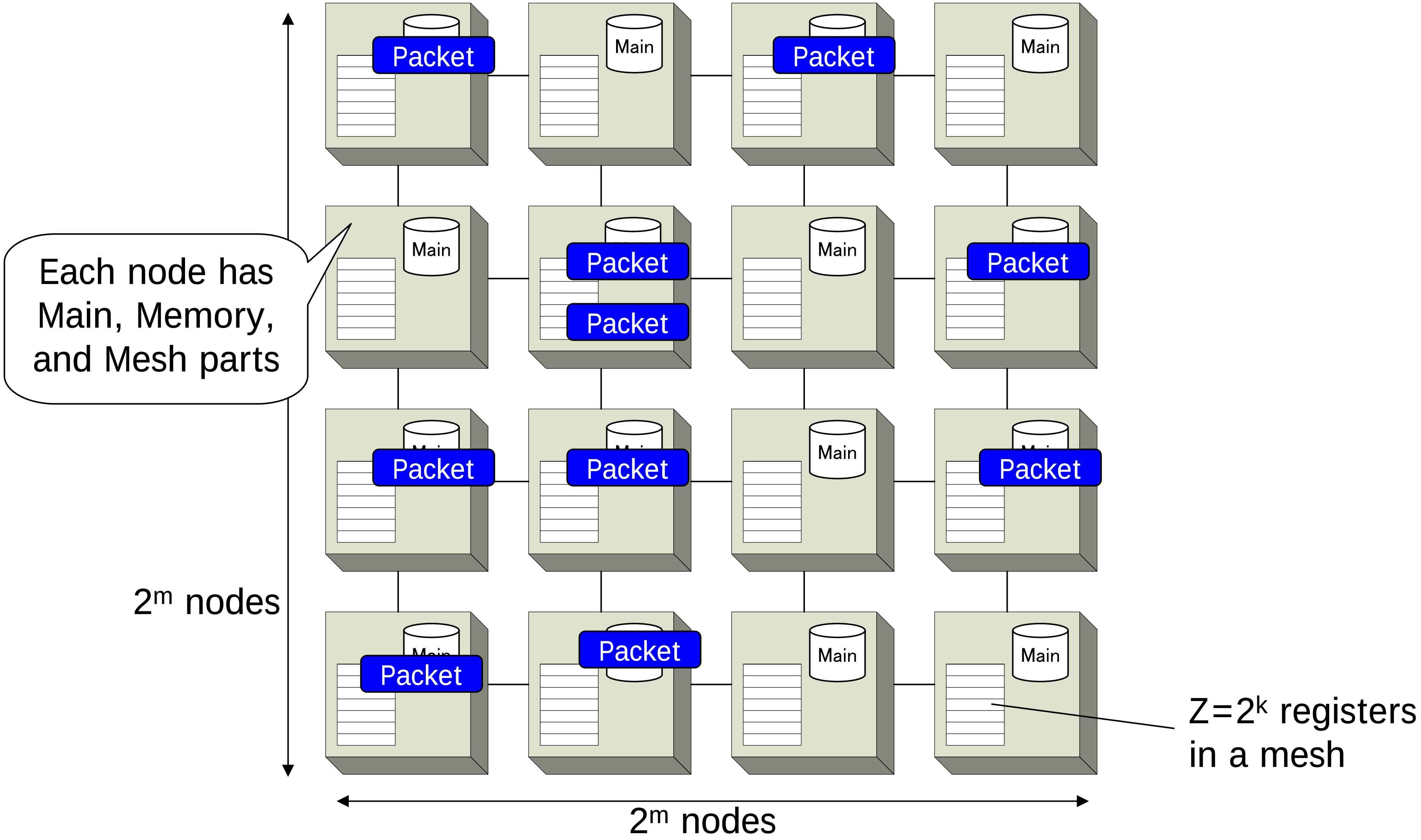
Aim of the Sieving

- To send all packets generated in the factor base to their target memory storage

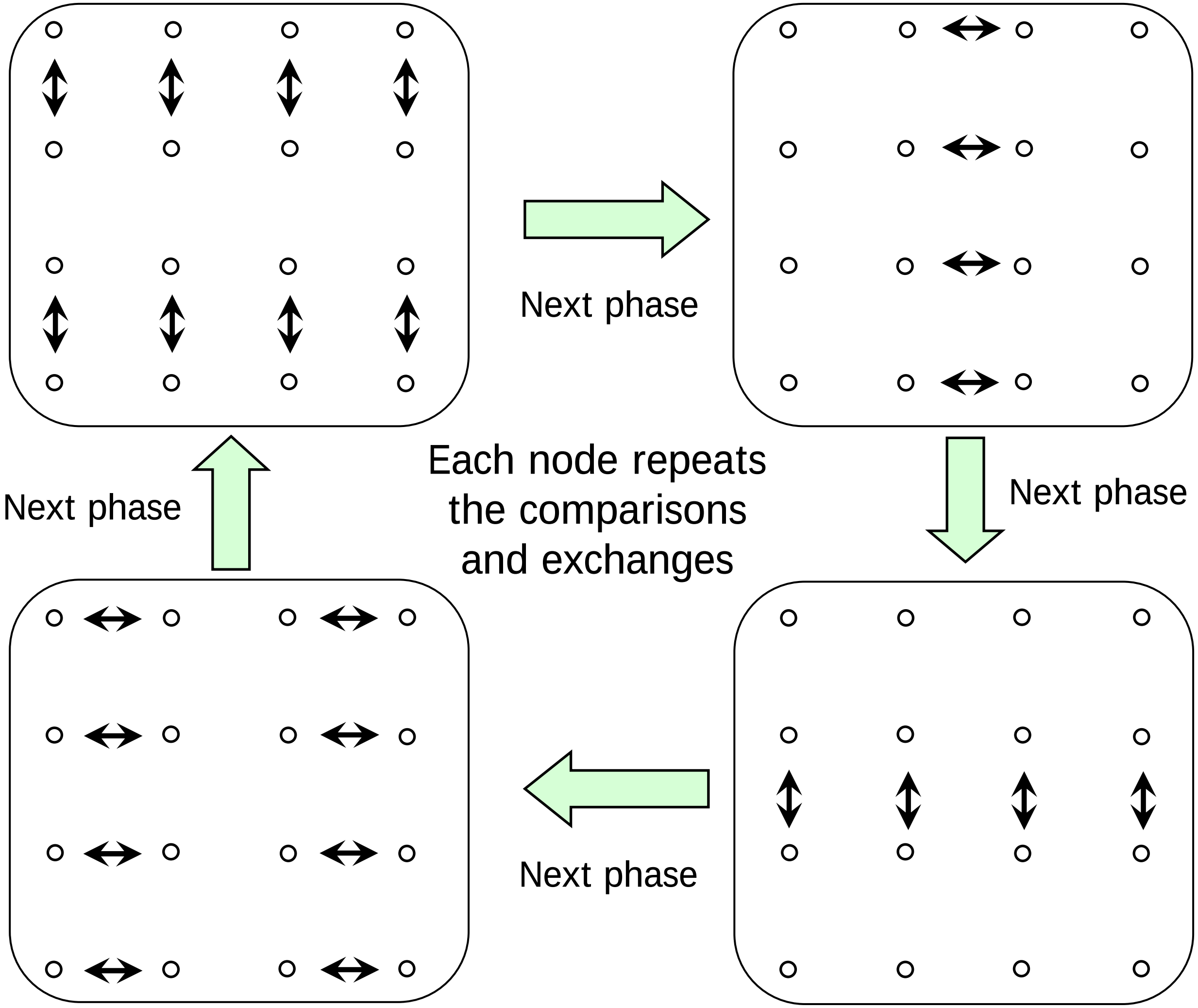


Mesh Structure

- YASD distributedly holds FB and memory storage in a mesh



Clockwise Transposition Routing



Each node repeats the comparisons and exchanges

The routing terminates in at most 2M steps experimentally

Evaluation of YASD768

- Optimized Parameters
  - k=24, m=8
- Chip Size
  - 49mm × 49mm ≒ 2400 mm^2
- Time
  - 1 subinterval is sieved in 40,000 clocks
  - All area is sieved in 12,500 days/set
  - Since 21 chips are obtained from 1 wafer, about 600 days are required for the sieving
- Assumptions
  - 130 nm technology
  - Frequency 500 MHz

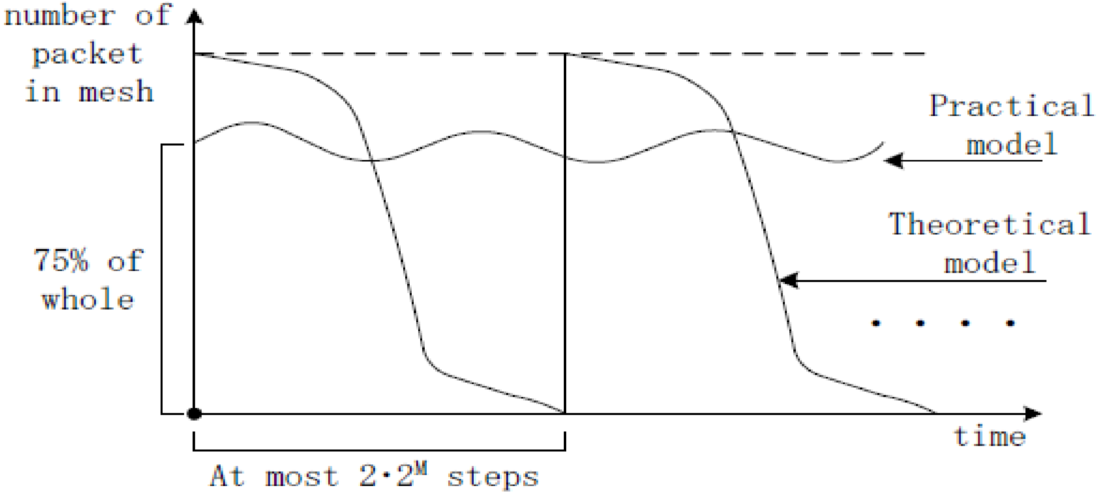
Contents

- Introduction
- Description of YASD
- Time Parameterization
- Area Parameterization
- Formulas and Optimizations
  - Generalized YASD
  - YASD for 768-bit Integers (YASD768)
  - YASD for 1024-bit Integers (YASD1024)
- Concluding Remarks

Required Time for Routing

- In Theory
  - Routing time in a $2^m \times 2^m$ mesh is at most 2×2^m

- In YASD
  - Above estimation cannot be applied directly, since packets are always sent from Main parts and to Memory parts
  - Thus we use a simplified model



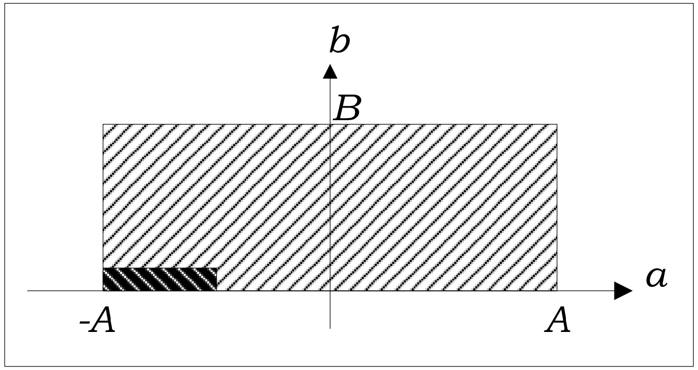
Time Parameterizations

Time for Routing

$$Time_{routing} = \frac{\displaystyle\sum_{2^{k-2m}<p<B_a} \frac{2^k}{p} + \sum_{2^{k-2m}<p<B_r} \frac{2^k}{p}}{2^m} \times \alpha \qquad (\alpha = 0.242)$$

Time for Sieving

$$Time^{(N)} = \frac{Time^{(N)}_{routing}}{500 \times 10^6} \times \frac{2Ha \times Hb}{2^k} \times \frac{3}{4} \times \frac{1}{365 \times 24 \times 3600} \text{[years]}$$



Contents

- Introduction
- Description of YASD
- Time Parameterization
- Area Parameterization
- Formulas and Optimizations
  - Generalized YASD
  - YASD for 768-bit Integers (YASD768)
  - YASD for 1024-bit Integers (YASD1024)
- Concluding Remarks

Details of YASD768

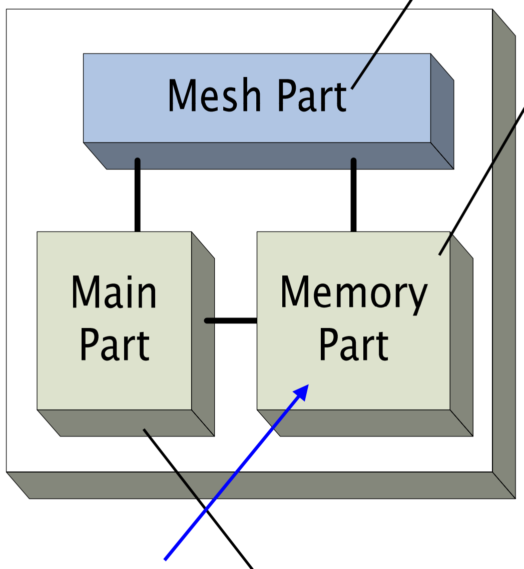
	# of Tr	# of DRAM
Main Part	2750	55000
Memory Part	1250	11500
Mesh Part	1100	
Total (in 1 node)	5100	66500

Tr　 : 2.8 [μm^2]
DRAM : 0.3 [μm^2]

- Since we have 256 × 256 nodes

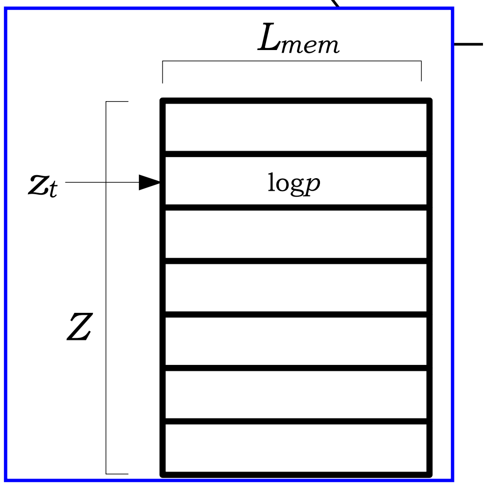
$$(5100 \times 2.8 + 66500 \times 0.3) \times 256 \times 256 = 2243.3\ \mathrm{mm}^2$$
$$\fallingdotseq 2400$$

Roles and Logics



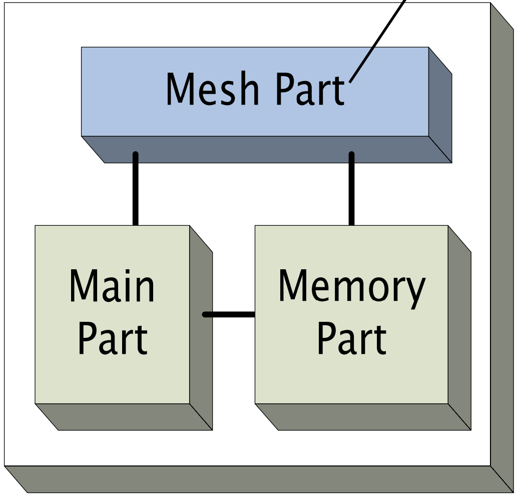
[Role] Comparing and exchanging packets
[Logic] Register, comparator

[Role] Adding log values to corresponding registers, storing sums and footprints
[Logic] Adder, buffers between Memory-Mesh Parts, circuits for final output, memory



[Role] Storing factor base, generating packets, sending packets to Mesh Parts
[Logic] Memory, adder, buffers between Main-Mesh Parts, circuits for initialization

Mesh Part

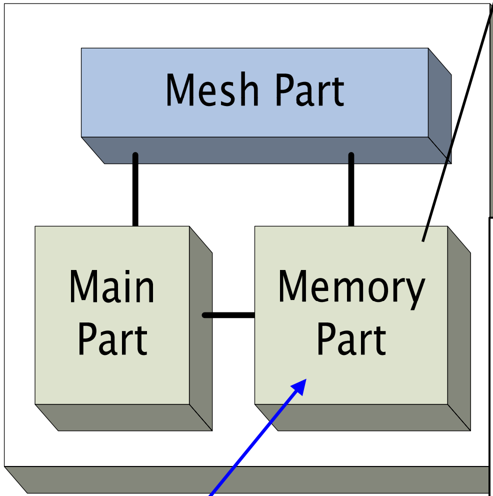


[Role] Comparing and exchanging packets

$$Tr_{mesh} = 2PAC \cdot H_{dff} + M \cdot H_{comp}$$

PAC	:	bit length of a packet
H_{dff}	:	#Tr of 1-bit D-F/F
M	:	bit length of coordinate values for repserenting a node
H_{comp}	:	#Tr for 1-bit comparator

Memory Part

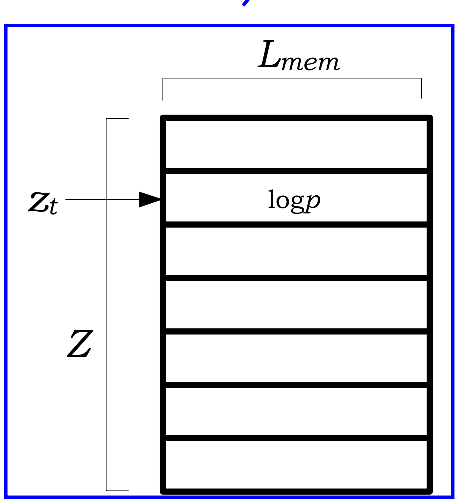


[Role] Adding log values to corresponding registers, storing sums and footprints

[Logic] Adder, buffer between Memory-Mesh Parts, circuit for final output, memory

$$Tr_{mem} = H_{add} \times L_{mem} + 2(PAC - 2M - 2) \times H_{latch} + 500$$

$$DRAM_{mem} = 2Z \cdot L_{mem} + \frac{F}{2^{2M}} L_{footprint} \times 1.3$$



H_{add}	:	#Tr for 1-bit adder
2^m	:	mesh size
PAC	:	bit length of a packet
H_{latch}	:	#Tr for 1-bit latch
z_t	:	target register

M

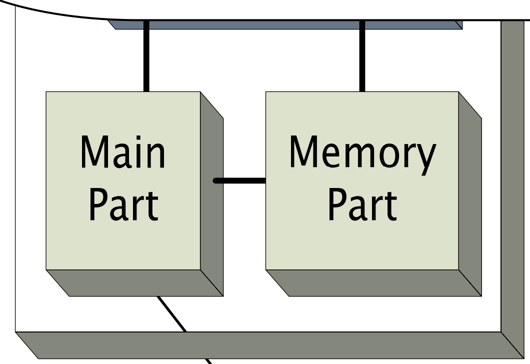
H_{add} : #Tr for 1-bit adder

L_p : bit length of a max prime

2^k : length of a subinterval

PAC : bit length of a packet

H_{latch} : #Tr of 1-bit latch



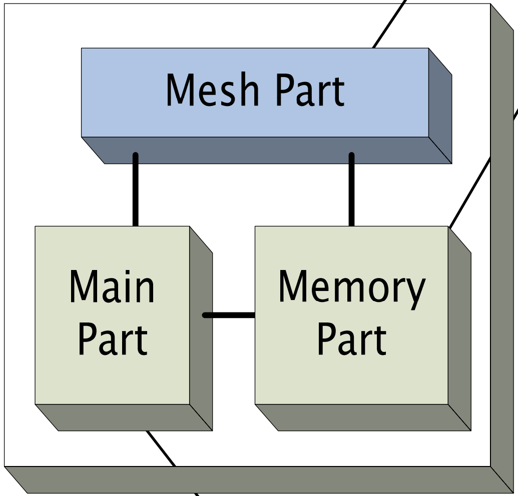
$$Tr_{main} = H_{add}\times\max(L_p,k)+2PAC\times H_{latch}+1000$$

$$DRAM_{main} = L_{fb}\times\frac{N}{2^{2M}}\times 1.1$$

[Role] Storing factor base, generating packets, sending packets to Mesh Parts

[Logic] Memory, adder, buffers between Main-Mesh Parts, circuits for initialization

DRAM



$$Tr_{mesh} = 2PAC \cdot H_{dff} + M \cdot H_{comp}$$

$$\begin{aligned} Tr_{mem} &= H_{add} \times L_{mem} + 2(PAC - 2M - 2) \\ &\quad \times H_{latch} + 500 \\ DRAM_{mem} &= 2Z \cdot L_{mem} + \frac{F}{2^{2M}} L_{\mathrm{footprint}} \times 1.3 \end{aligned}$$

[Ro

[Lo

$$\begin{aligned} Tr_{main} &= H_{add} \times \max(L_p, k) + \\ &\quad 2PAC \times H_{latch} + 1000 \\ DRAM_{main} &= L_{fb} \times \frac{N}{2^{2M}} \times 1.1 \end{aligned}$$

esh

Contents

- Introduction
- Description of YASD
- Parametarization
- Formulas and Optimizations
  - Generalized YASD
  - YASD for 768-bit Integers (YASD768)
  - YASD for 1024-bit Integers (YASD1024)
- Concluding Remarks

Formulas for Generalized YASD

FUJITSU

$$
\begin{aligned}
Area^{(N)} &= Tr_{main} + Tr_{mem} + Tr_{mesh} + DRAM_{main} + DRAM_{mem} \\
&= \{(190.4m + 201.6k + 89.6L_{\log} + 112L_{mem} + 7320) \times 2^{2m} \\
&\qquad + (0.33nL_{fb} + 0.3 \times 2^{k+1} L_{mem} + (1.3k + 15.6)F)\,[\mu\mathrm{m}^2]
\end{aligned}
$$

$$
Time^{(N)}_{routing} = \left(\sum_{p>2^{k-2m}}^{Ba} \frac{2^k}{p} + \sum_{p>2^{k-2m}}^{Br} \frac{2^k}{p} \right) \times \frac{0.24}{2^m}
$$

$$
Time^{(N)} = \frac{Ha \times Hb}{1.83 \times 10^{17}} \times Time^{(N)}_{routing}
$$

Circuit Parameters

		768-bit	1024-bit
L_p	Bit length of max prime	30	32
L_{log}	Bit length of int(log(p))	6	8
L_{mem}	Bit length of Σ int(log(p))	10	11
n	# of primes	7.97×10^7	1.32×10^9
F	# of footprints	0.496×2^k	0.818×2^k
L_{fb}	average bit length of a prime	38	42
H_{add}	1-bit adder	40 Tr	
H_{dff}	1-bit D-F/F	8 Tr	
H_{latch}	1-bit latch	4 Tr	
H_{comp}	1-bit comparator	20 Tr	

Sieving Parameters

	768-bit	1024-bit
B_r	10^8	3.5×10^9
B_a	10^9	2.6×10^{10}
$2Ha$	3.4×10^{13}	1.1×10^{15}
Hb	8.9×10^6	2.7×10^8

Formulas for YASD768

FUJITSU

$$Area^{(768)}(k,m) = \{(190.4m + 201.6k + 8977.6)\times 2^{2m}$$

$$+(0.645k + 13.74)\times 2^{k} + 9.99\times 10^{8}\ [\mu\mathrm{m}^2]$$

$$Time^{(768)}_{routing}(k,m) = \left(5.94 - 2\log\log 2^{k-2m}\right)\times\frac{0.24}{2^m}$$

$$Time^{(768)}(k,m) = 3453\times\frac{5.94 - 2\log\log 2^{k-2m}}{2^m}[\mathrm{years}]$$

- Optimized Parameters (w.r.t AT-product): k=24, m=8

$$Area^{(768)}(24,8) = 2500 \quad [\mathrm{mm}^2]$$

$$Time^{(768)}(24,8) = 34 \quad [\mathrm{years}]$$

AT Products of YASD768

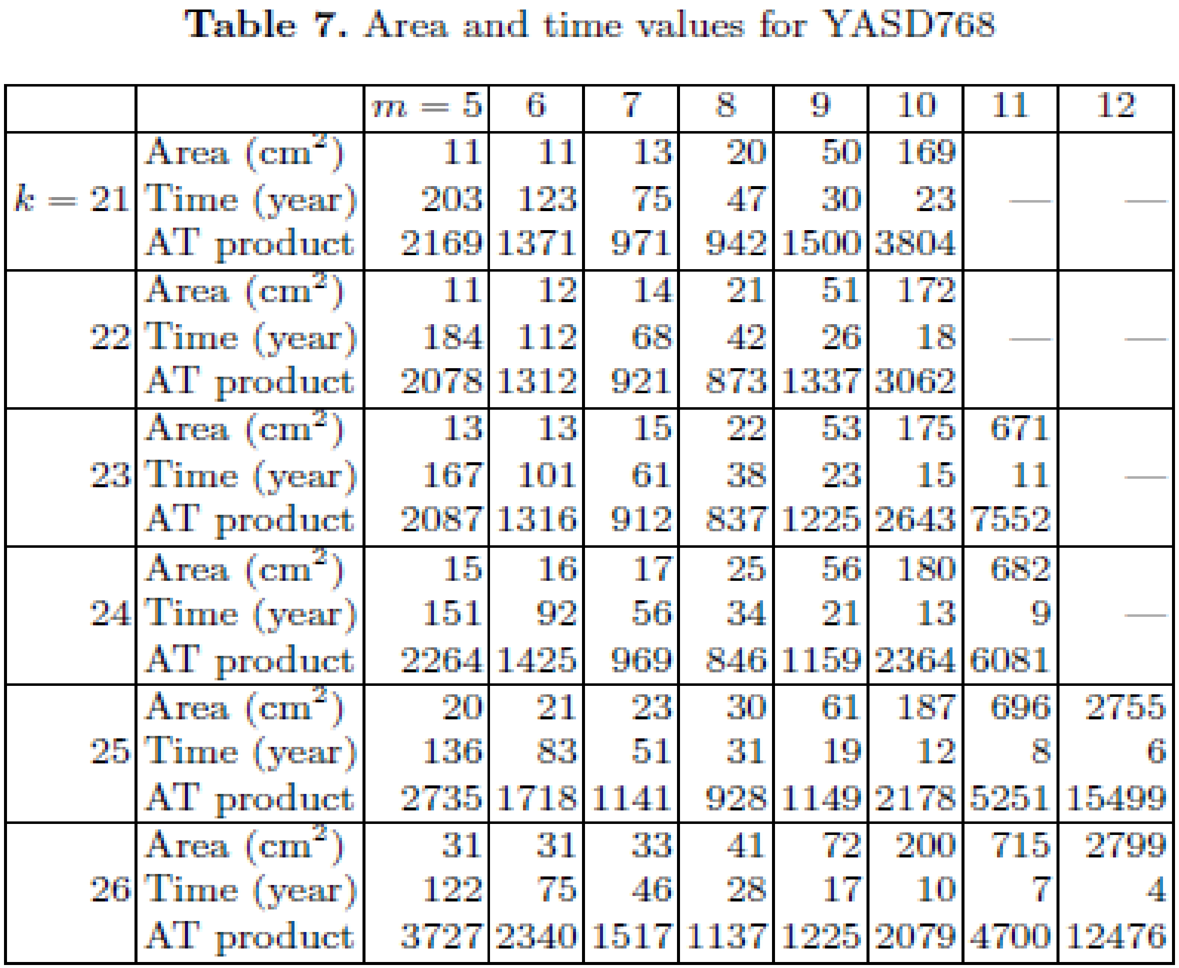


Table 7. Area and time values for YASD768

		$m = 5$	6	7	8	9	10	11	12
$k = 21$	Area (cm^2)	11	11	13	20	50	169		
	Time (year)	203	123	75	47	30	23	—	—
	AT product	2169	1371	971	942	1500	3804		
22	Area (cm^2)	11	12	14	21	51	172		
	Time (year)	184	112	68	42	26	18	—	—
	AT product	2078	1312	921	873	1337	3062		
23	Area (cm^2)	13	13	15	22	53	175	671	
	Time (year)	167	101	61	38	23	15	11	—
	AT product	2087	1316	912	837	1225	2643	7552	
24	Area (cm^2)	15	16	17	25	56	180	682	
	Time (year)	151	92	56	34	21	13	9	—
	AT product	2264	1425	969	846	1159	2364	6081	
25	Area (cm^2)	20	21	23	30	61	187	696	2755
	Time (year)	136	83	51	31	19	12	8	6
	AT product	2735	1718	1141	928	1149	2178	5251	15499
26	Area (cm^2)	31	31	33	41	72	200	715	2799
	Time (year)	122	75	46	28	17	10	7	4
	AT product	3727	2340	1517	1137	1225	2079	4700	12476

Formulas for YASD1024

$$Area^{(1024)}(k,m) = \{(190.4m + 201.6k + 9268.8)\times 2^{2m}$$

$$+(1.06k + 19.36)\times 2^{k} + 1.83\times 10^{10}\ [\mu m^{2}]$$

$$Time^{(1024)}_{routing}(k,m) = \left(6.27 - 2\log\log 2^{k-2m}\right)\times \frac{0.24}{2^{m}}$$

$$Time^{(1024)}(k,m) = 339041\times \frac{6.27 - 2\log\log 2^{k-2m}}{2^{m}}[\text{years}]$$

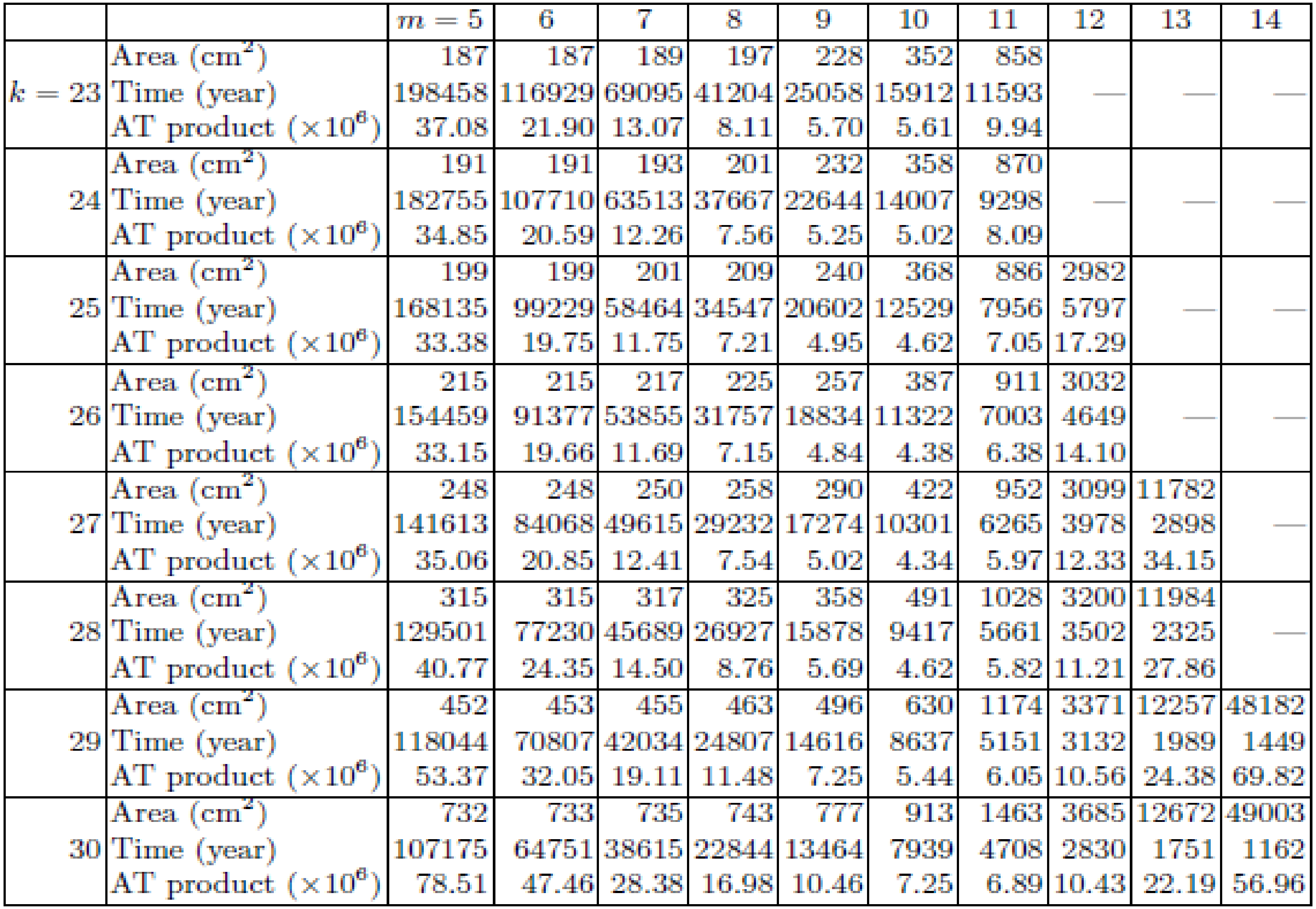
- Optimized Parameters (w.r.t AT-product): k=27,m=10

$$Area^{(1024)}(27,10) = 42200 \quad [\text{mm}^{2}]$$

$$Time^{(1024)}(27,10) = 10301 \quad [\text{years}]$$

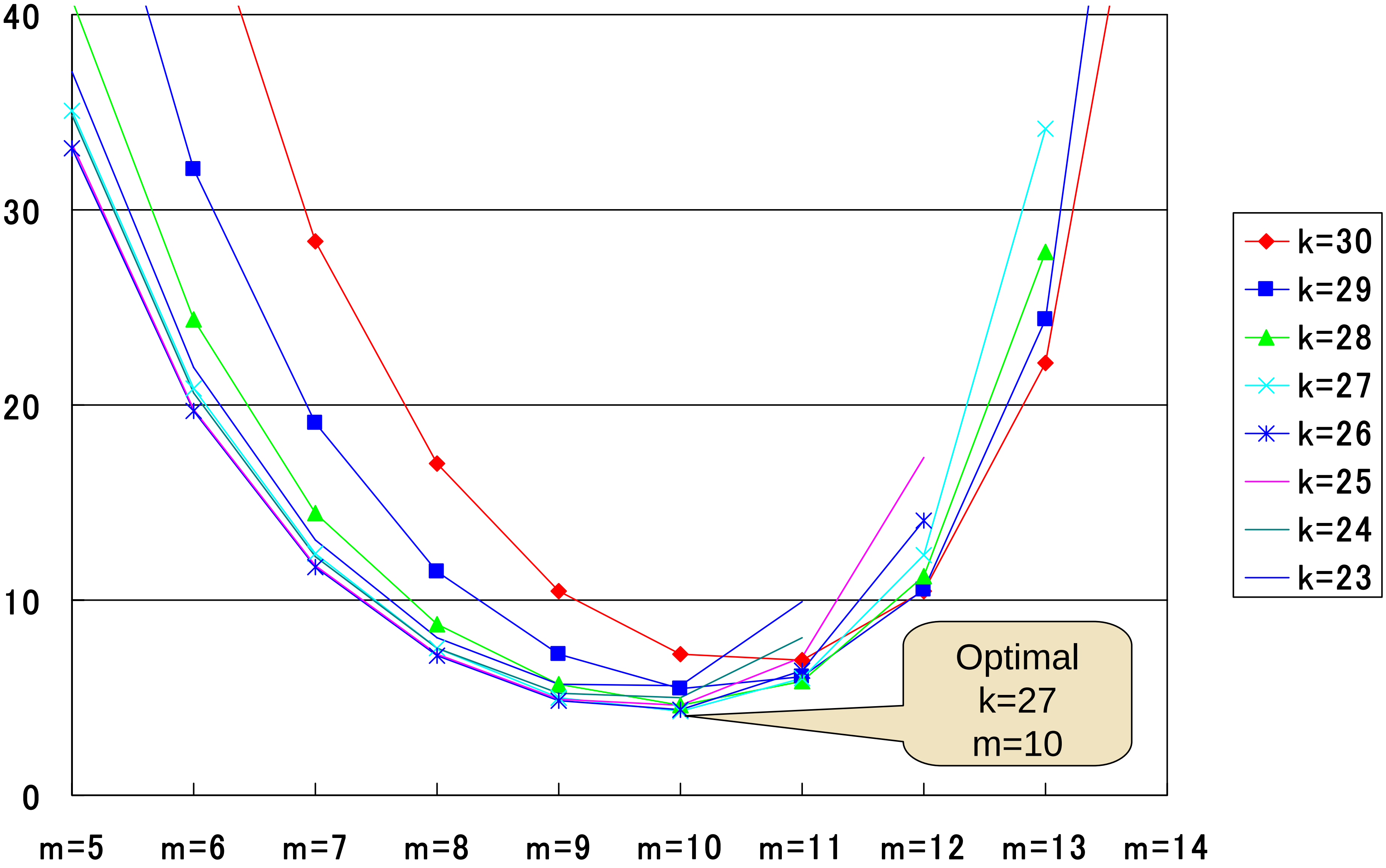
AT Products of YASD1024

Table 6. Area and time values for YASD1024



		$m = 5$	6	7	8	9	10	11	12	13	14
	Area (cm^2)	187	187	189	197	228	352	858			
$k = 23$	Time (year)	198458	116929	69095	41204	25058	15912	11593	—	—	—
	AT product ($\times 10^6$)	37.08	21.90	13.07	8.11	5.70	5.61	9.94			
	Area (cm^2)	191	191	193	201	232	358	870			
24	Time (year)	182755	107710	63513	37667	22644	14007	9298	—	—	—
	AT product ($\times 10^6$)	34.85	20.59	12.26	7.56	5.25	5.02	8.09			
	Area (cm^2)	199	199	201	209	240	368	886	2982		
25	Time (year)	168135	99229	58464	34547	20602	12529	7956	5797	—	—
	AT product ($\times 10^6$)	33.38	19.75	11.75	7.21	4.95	4.62	7.05	17.29		
	Area (cm^2)	215	215	217	225	257	387	911	3032		
26	Time (year)	154459	91377	53855	31757	18834	11322	7003	4649	—	—
	AT product ($\times 10^6$)	33.15	19.66	11.69	7.15	4.84	4.38	6.38	14.10		
	Area (cm^2)	248	248	250	258	290	422	952	3099	11782	
27	Time (year)	141613	84068	49615	29232	17274	10301	6265	3978	2898	—
	AT product ($\times 10^6$)	35.06	20.85	12.41	7.54	5.02	4.34	5.97	12.33	34.15	
	Area (cm^2)	315	315	317	325	358	491	1028	3200	11984	
28	Time (year)	129501	77230	45689	26927	15878	9417	5661	3502	2325	—
	AT product ($\times 10^6$)	40.77	24.35	14.50	8.76	5.69	4.62	5.82	11.21	27.86	
	Area (cm^2)	452	453	455	463	496	630	1174	3371	12257	48182
29	Time (year)	118044	70807	42034	24807	14616	8637	5151	3132	1989	1449
	AT product ($\times 10^6$)	53.37	32.05	19.11	11.48	7.25	5.44	6.05	10.56	24.38	69.82
	Area (cm^2)	732	733	735	743	777	913	1463	3685	12672	49003
30	Time (year)	107175	64751	38615	22844	13464	7939	4708	2830	1751	1162
	AT product ($\times 10^6$)	78.51	47.46	28.38	16.98	10.46	7.25	6.89	10.43	22.19	56.96

AT Products of YASD1024



Optimal
k=27
m=10

Optimized YASD1024

- Optimized Parameters: k=27, m=10
  - Area: 42200 mm^2
  - Time: 10301 years (by 1set)
  - Cost: 3200 USD (excluding NRE, defects and power supply)

- Even if we use 600 wafers (like TWIRL1024), more than 17 years are required

- Since we did not consider the wiring problem and the mini-factoring problem, YASD1024 will require more area and time.

Concluding Remarks

- Established general formulas for generalized YASD
  - Area
  - Time
- Evaluated the performance of YASD1024
  - k=27, m=10
  - Area: 42200 mm^2
  - Time: 10301 years (1set)
  - Cost: 3200 USD (excluding NRE, defects and power supply)

- Future Works
  - Consider the wiring problem
  - Application of ECM to the mini-factoring part

FUJITSU

THE POSSIBILITIES ARE INFINITE