An Energy-Efficient IEEE 1363-based Reconfigurable Public-Key Cryptograph Processor

James Goodman
Chrysalis-ITS

Anantha Chandrakasan
Massachusetts Institute of Technology

Standardization, or lack th

- **No single dominant standard as in symmetric key**

- **IEEE 1363-2000 Public Key Cryptography Standard**
  - ⇒ **IF: Integer Factorization (e.g., RSA)**
  - ⇒ **DL: Discrete Logarithms (e.g., DH and DSA)**
  - ⇒ **ECDL: Elliptic Curve Discrete Logarithms (e.g., ECDSA)**

- **Choices can lead to incompatibilities**

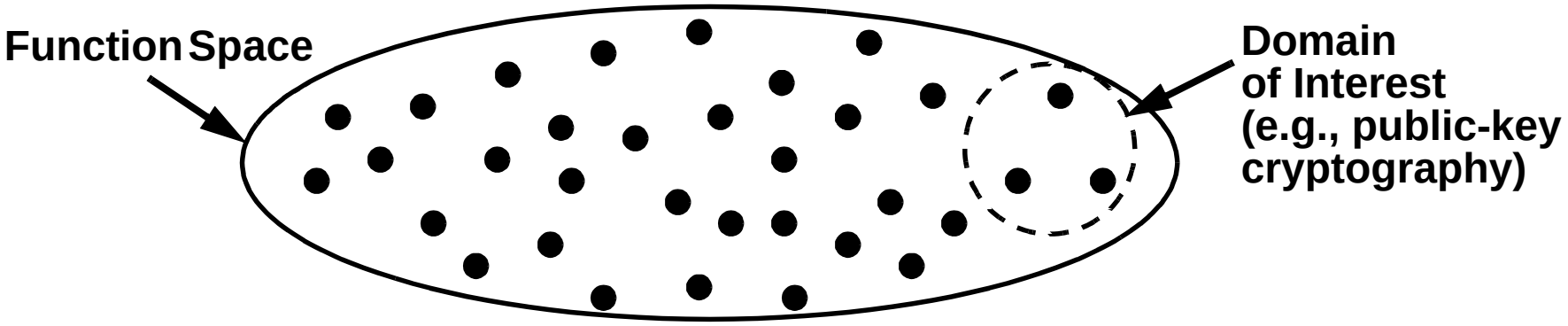
Algorithm agility required to ensure compatibility

Comparison of Conventional Solutions

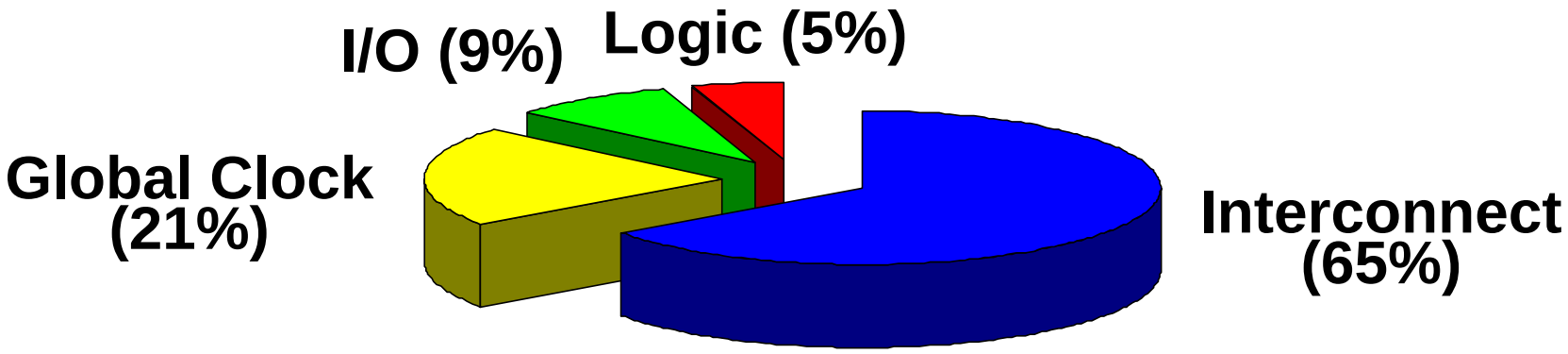
	Energy Efficiency	Performance	Design Effort/Cost	Reconfiguration Cost
Software	low	low	low	low
Dedicated Hardware	high	high	high	∞
Programmable Hardware	med	med/high	med	med
The Panacea	high	high	low	low

SOLUTION: Domain Specific Reconfigurable Cryptographic Processor

Cost of Reconfigurable Computing



- **Energy efficiency suffers due to their flexibility:**



[Kusse'98]

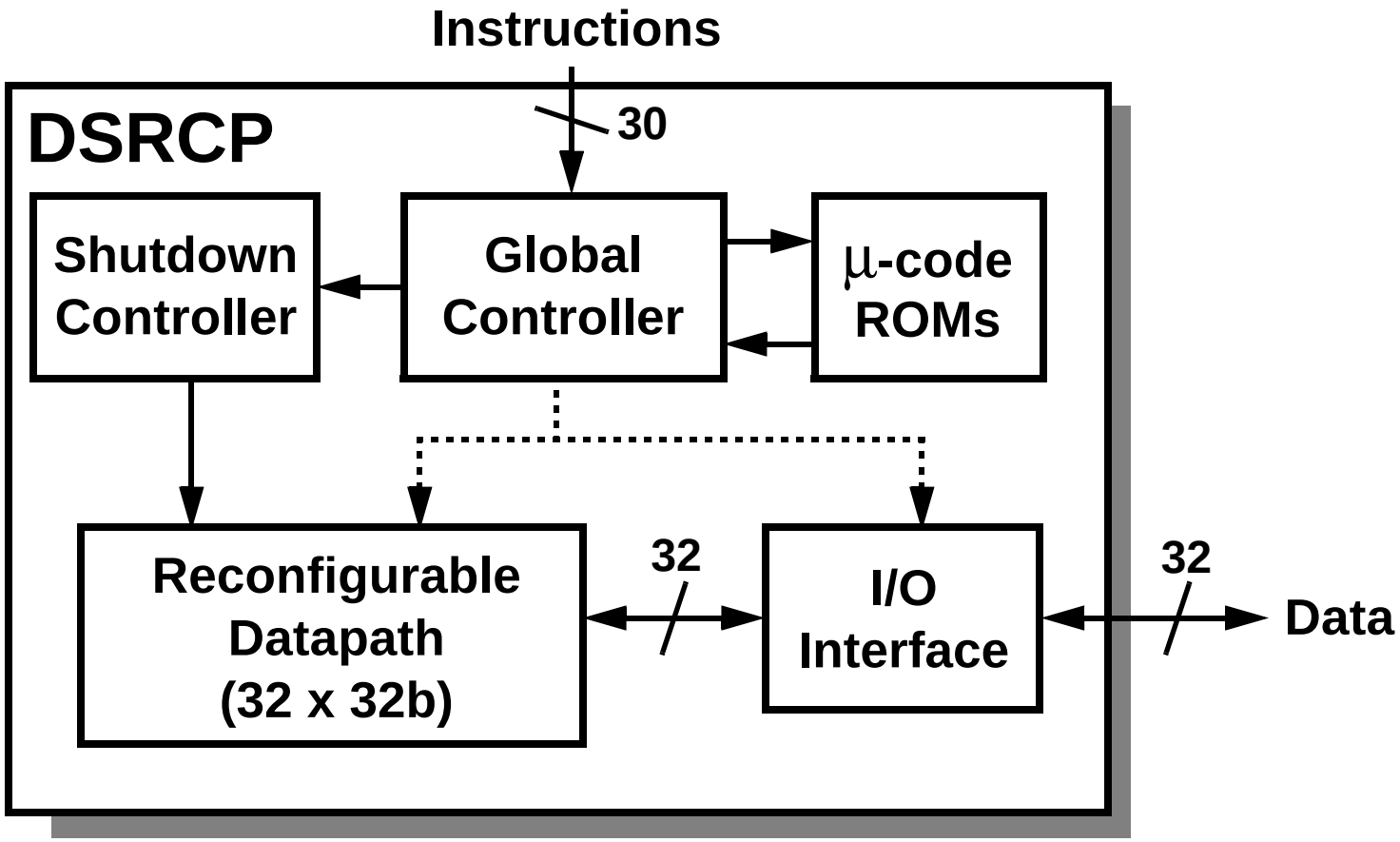
Our focus: interconnect-centric architecture

Instruction Set Definition

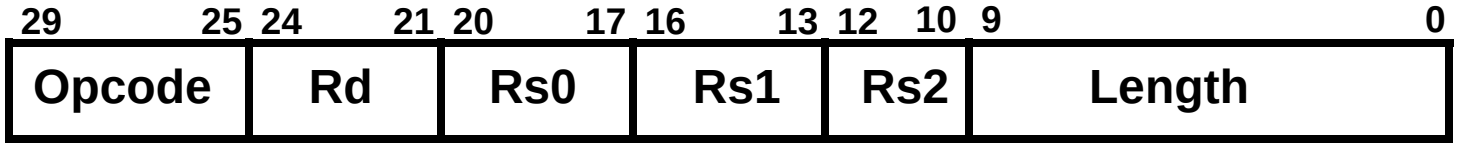
- **Instruction matrix derived from IEEE 1363-2000**

	ADD	SUB	MULT	MOD	MOD_ADD	MOD_SUB	MOD_MULT	MOD_INV	MOD_EXP	GF_ADD	GF_MULT	GF_SQR	GF_INV	GF_EXP	EC_ADD	EC_DOUBLE	EC_MULT
PKO #1									X								
PKO #2			X		X	X	X		X								
IFEP-RSA									X								
IFDP-RSA			X		X	X	X		X								
IFSP-RSA1			X		X	X	X		X								
IFVP-RSA1									X								
DLSVDP-DH														X			
DLSVDP-MQV	X				X		X				X			X			
DLSP-DSA				X	X		X	X									
DLVP-DSA				X			X	X						X			
ECSVDP-DH																	X
ECSVDP-MQV					X		X								X		X
ECSP-DSA				X	X		X	X									
ECVP-DSA				X			X	X							X		X
EC_ADD										X	X	X	X				
EC_DOUBLE										X	X		X				
EC_MULT															X	X	

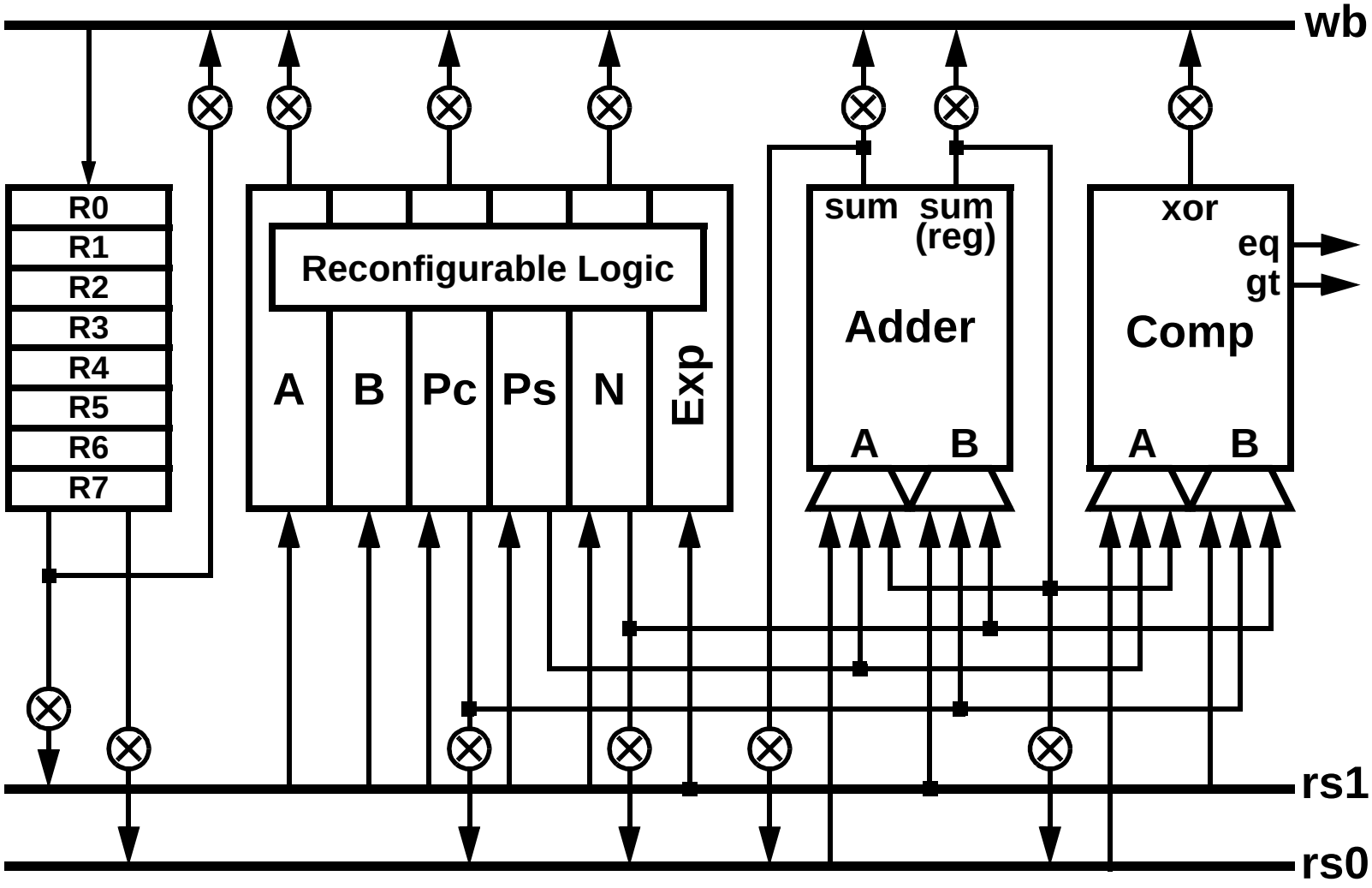
Top Level Arch



- **Instruction format:**



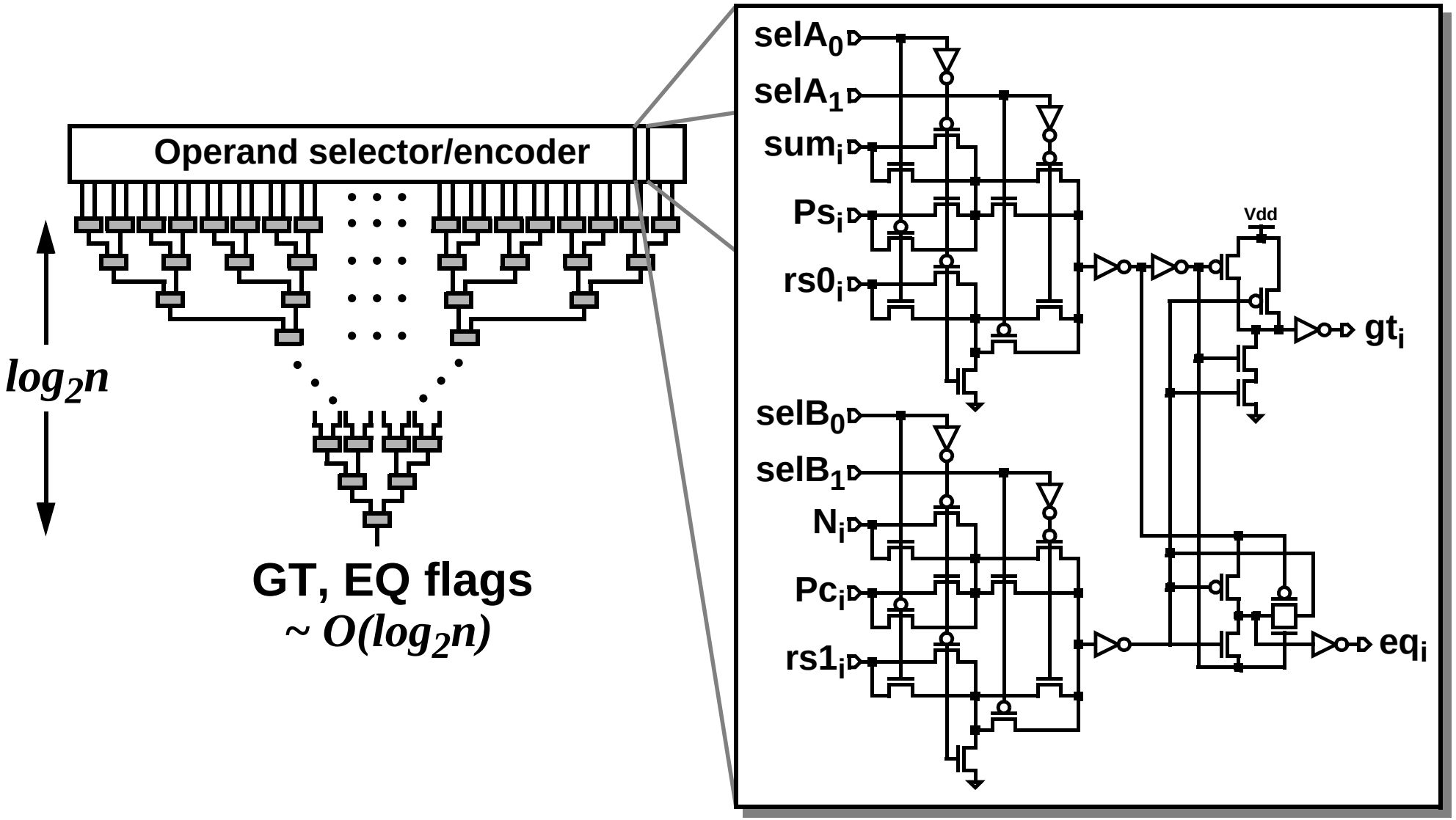
Reconfigurable Datapath



- Reprogrammable interconnect is predominantly local interconnect

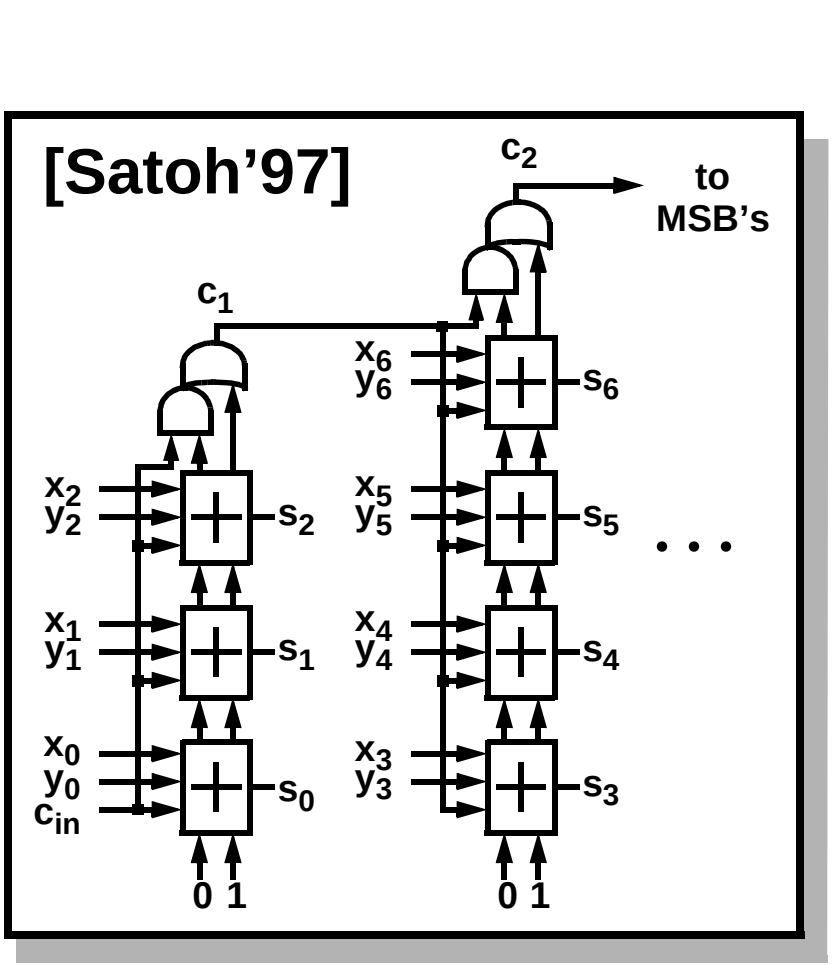
Comparator Module

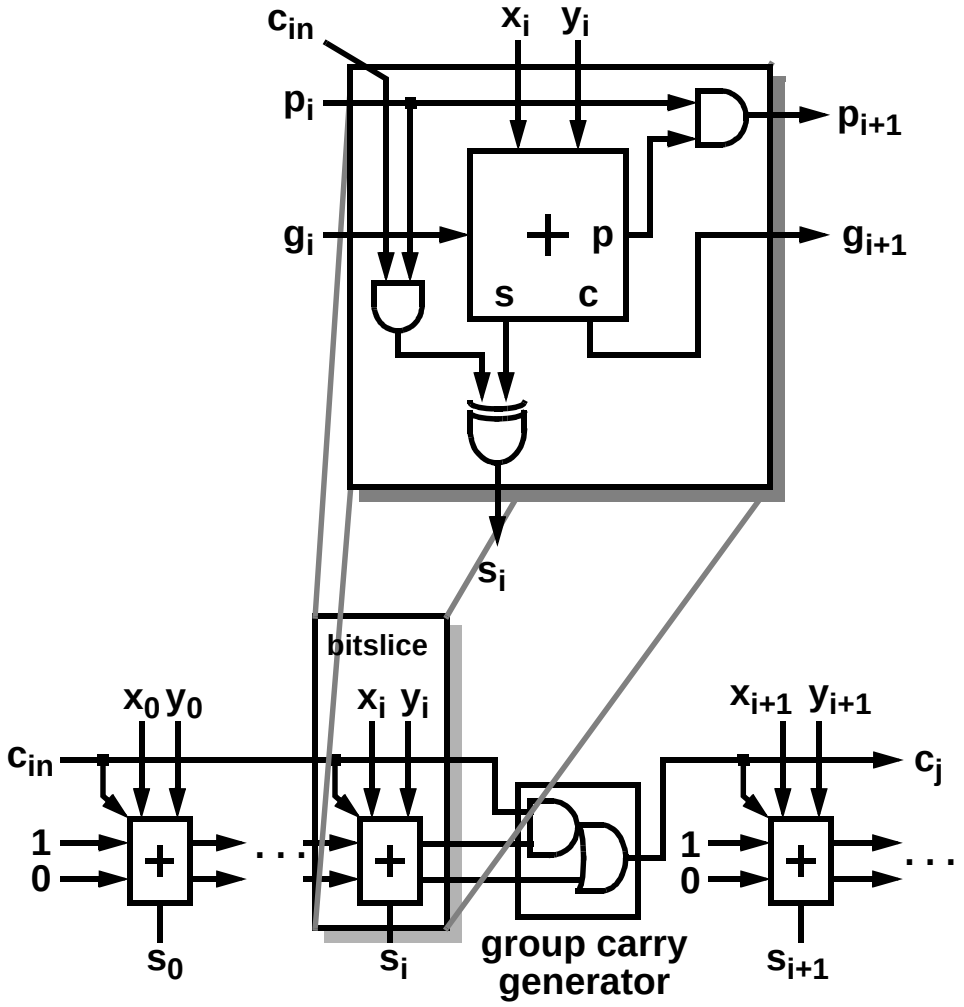
- Operand size requires fast comparator



Wide Adder Module

- **Combined carry-select & carry-bypass technique**
  - ⇒ **3 cycle latency for 1024 bit operation**





Reconfigurable Datapath

- **Montgomery Multiplication**

$$\Rightarrow (Pc,Ps)_j = \frac{(Pc,Ps)_{j-1} + b_jA + q_jN}{2}$$

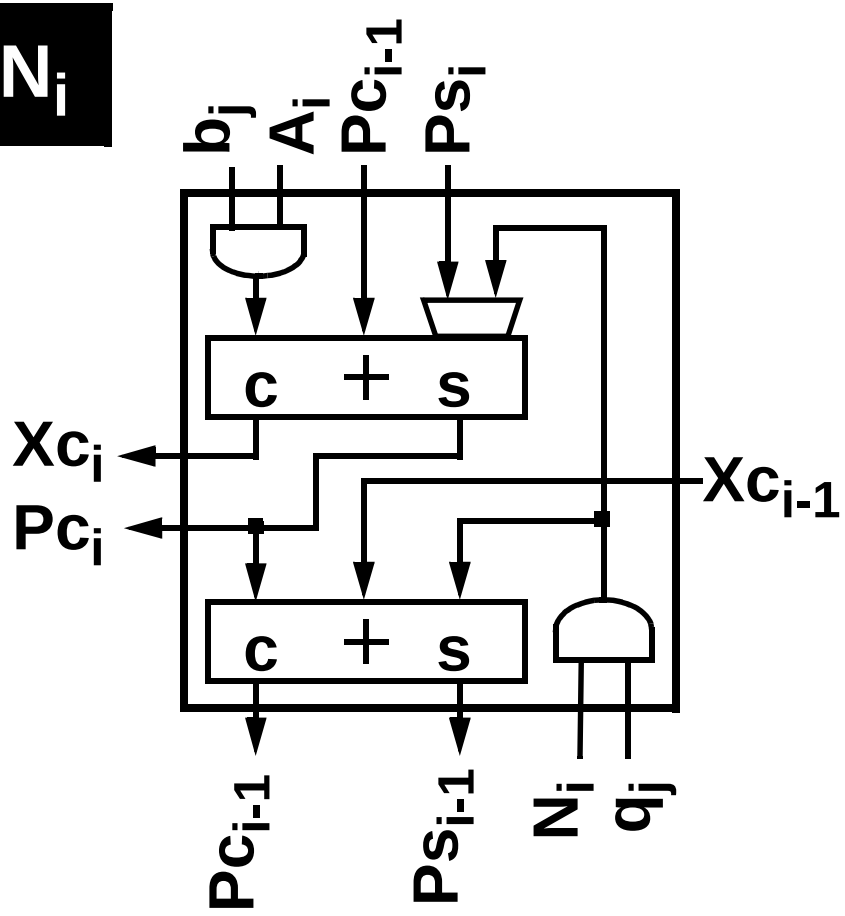
$$(Pc,Ps)_{i-1} = (Pc,Ps)_i + b_jA_i + q_jN_i$$

- **MSB-first GF(2^n) Multiplication**

$\Rightarrow P_j = 2P_{j-1} + b_jA + q_jN$

$\Rightarrow$ FA sum = a Å b Å cin

$$Pc_i = Pc_{i-1} + b_jA_i + q_jN_i$$



GF(2^n) Inverter Configuration

- **Inversion performance dominates EC operations**
  - ⇒ **combine invert and multiply for 18% improvement**

- **Extended Euclidean Algorithm:**

  N = *f(x)* Ps = *f(x)* A = 0

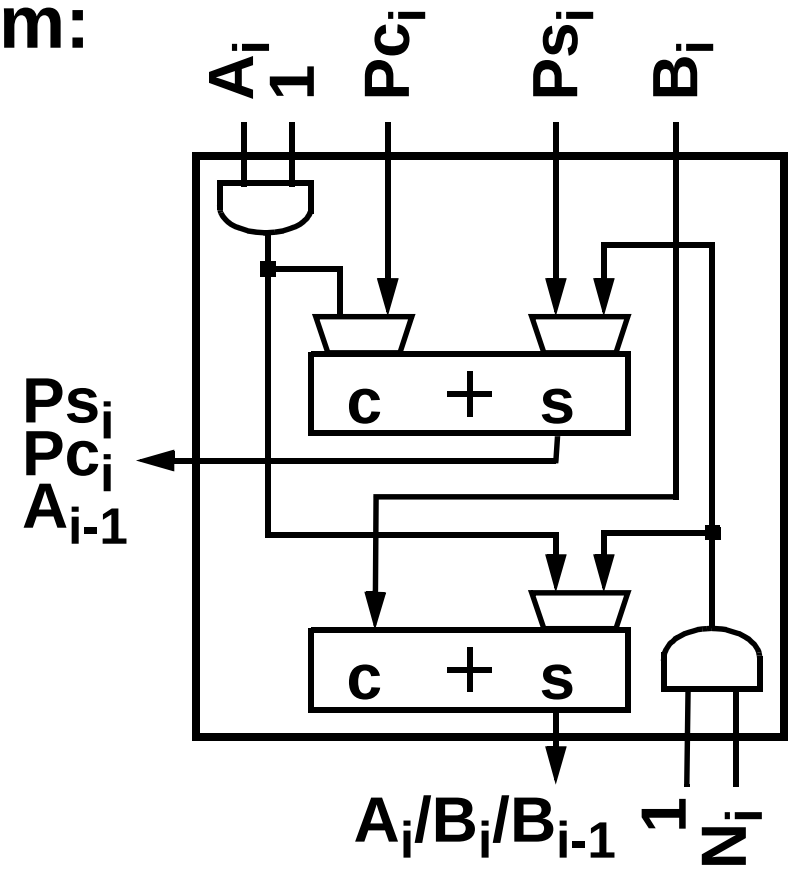
  Pc = 0 B = 1 or b

- **At completion:**

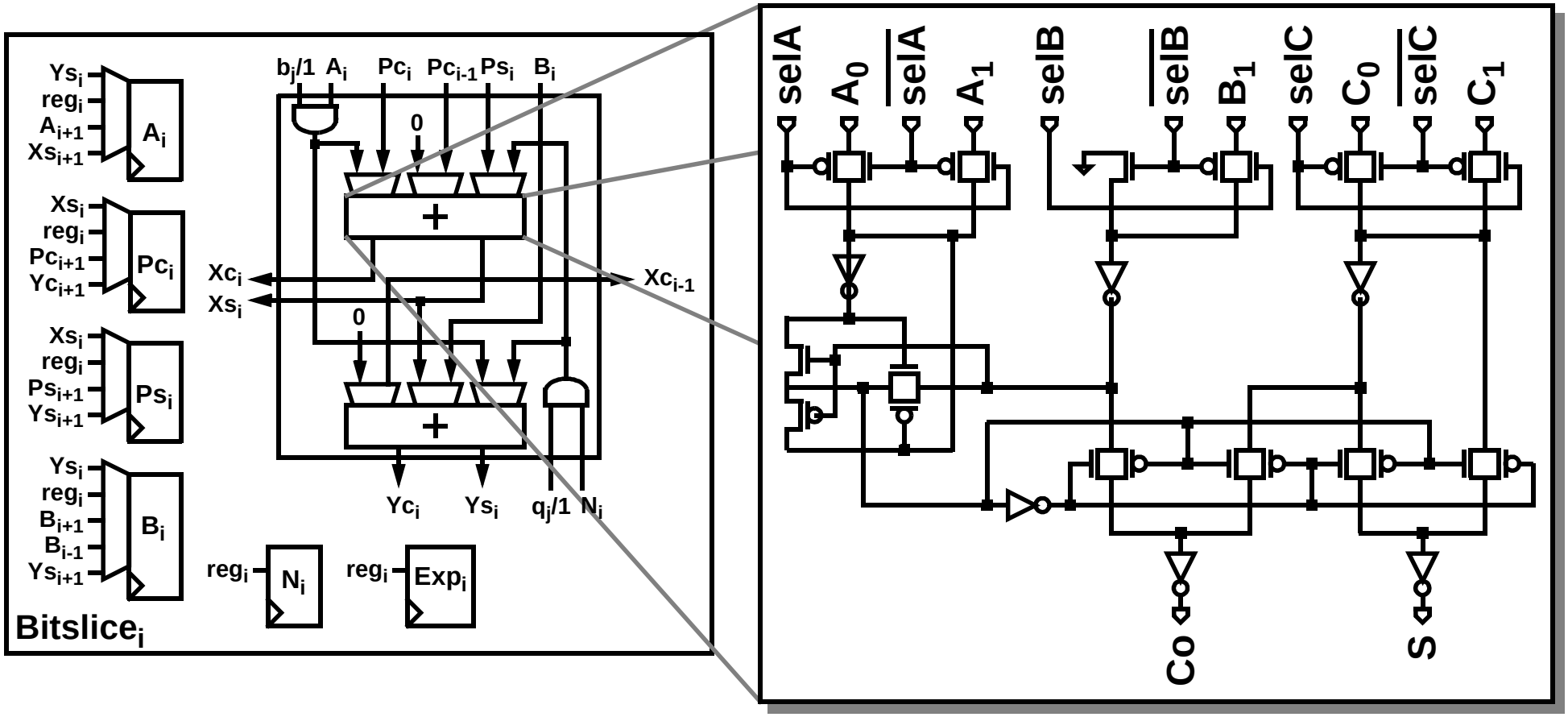
  A = 1/a (B = 1 initially)

  A = b/a (B = b initially)

Maps to same H/W as multipliers

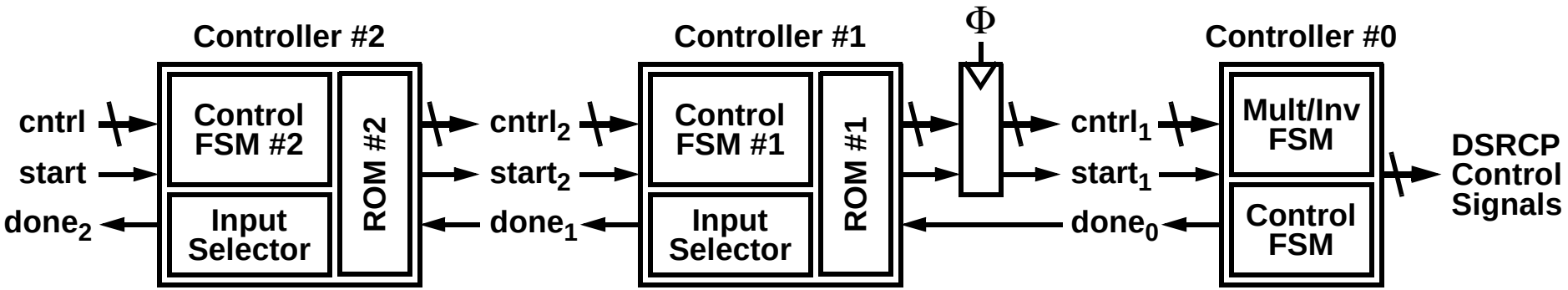


Final Reconfigurable Bitslice Design



- **Minimal global interconnect**
  - ⇒ **5 register selects + 3 adder selects + 6 clocks**

Controller Design

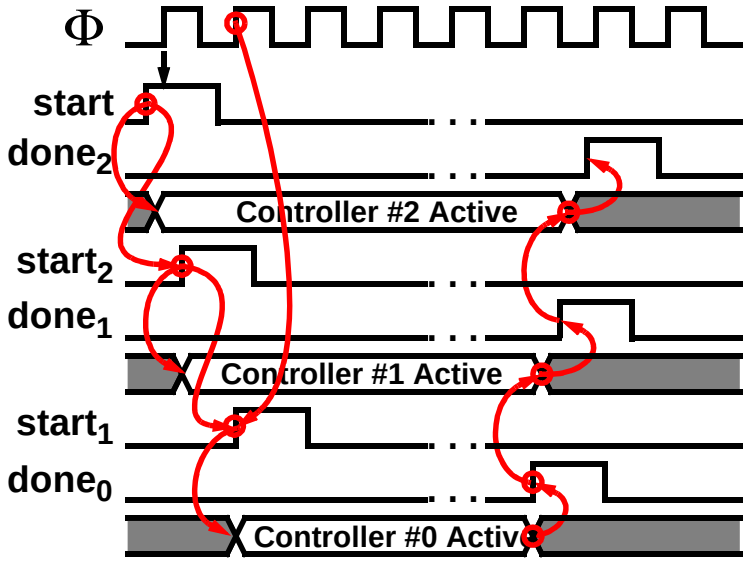


- **3 levels of control**

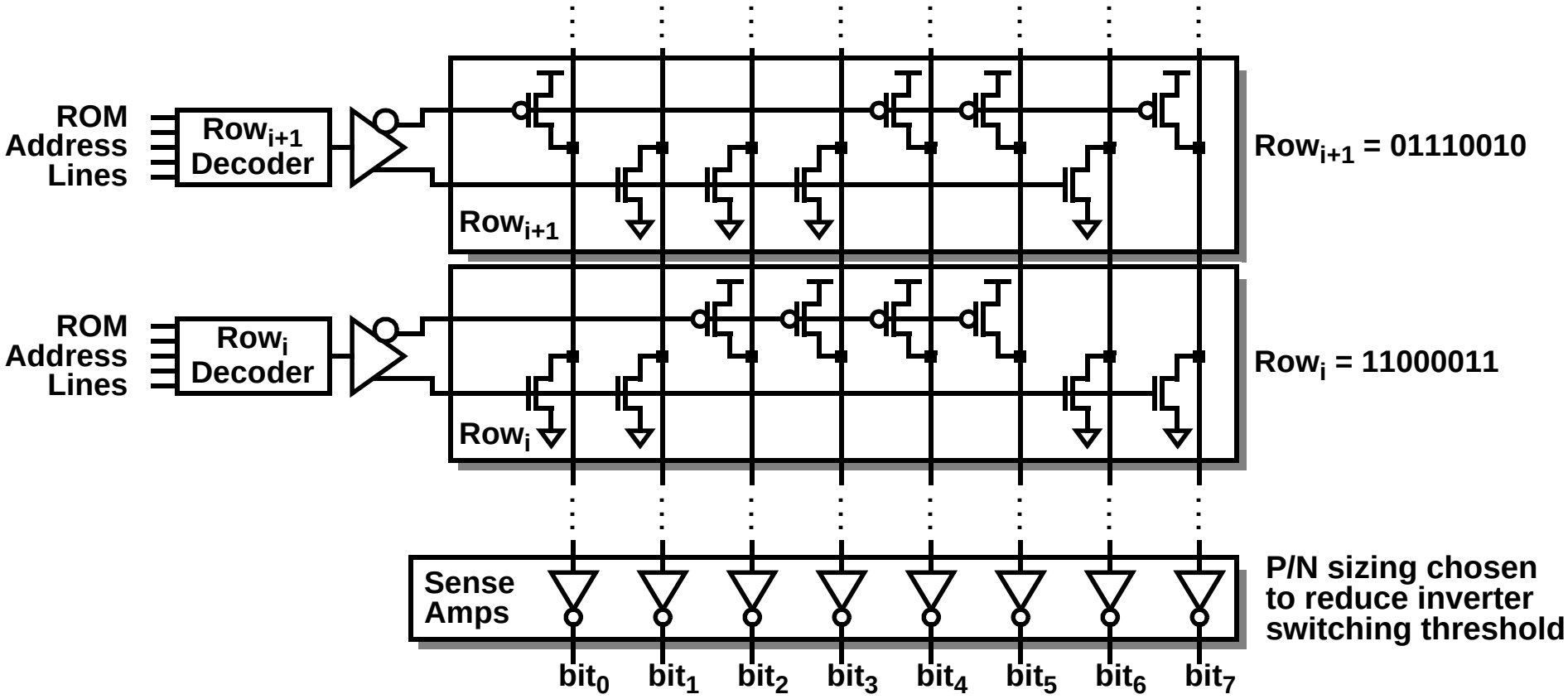
⇒ **Level 0:** ADD, SUB, COMP
GF(invert,invmult,mult,add)
MONT(mult,reduce)
SET_LENGTH

⇒ **Level 1:** MOD(add,sub)
GFexp
EC(add,double)

⇒ **Level 2:** MOD(mult,exp,invert)
ECmult

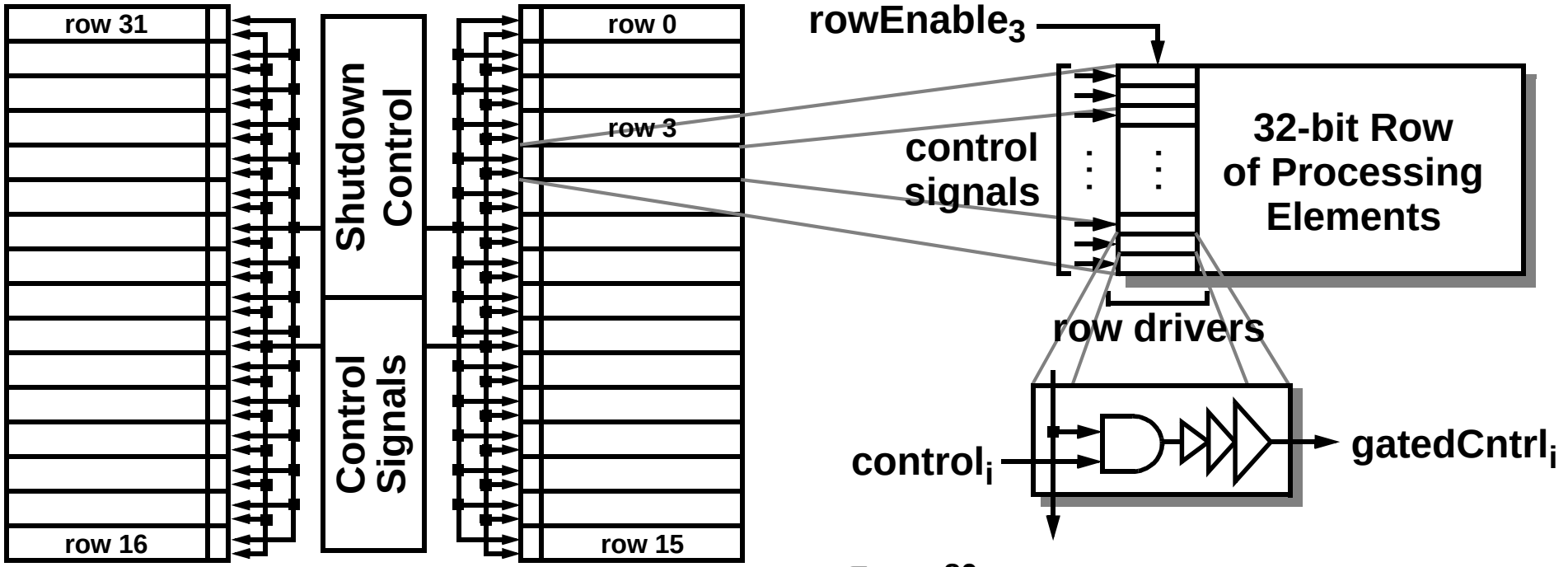


Static Microcode ROMs

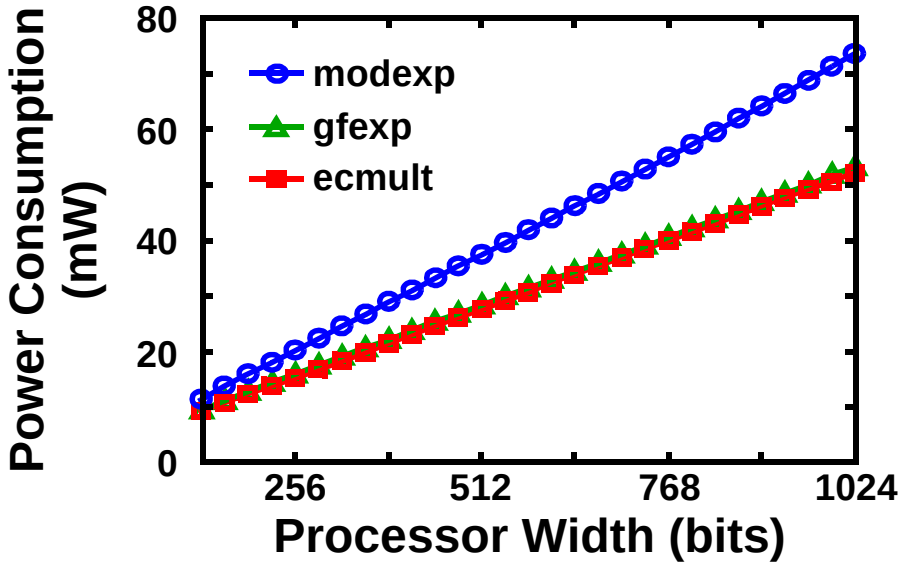


- **Overhead = twice the number of row select lines**
  - ⇒ **+10% energy/ROM**
  - ⇒ **<< 1% energy/chip (operation dependent)**

Clock Gating Strategy

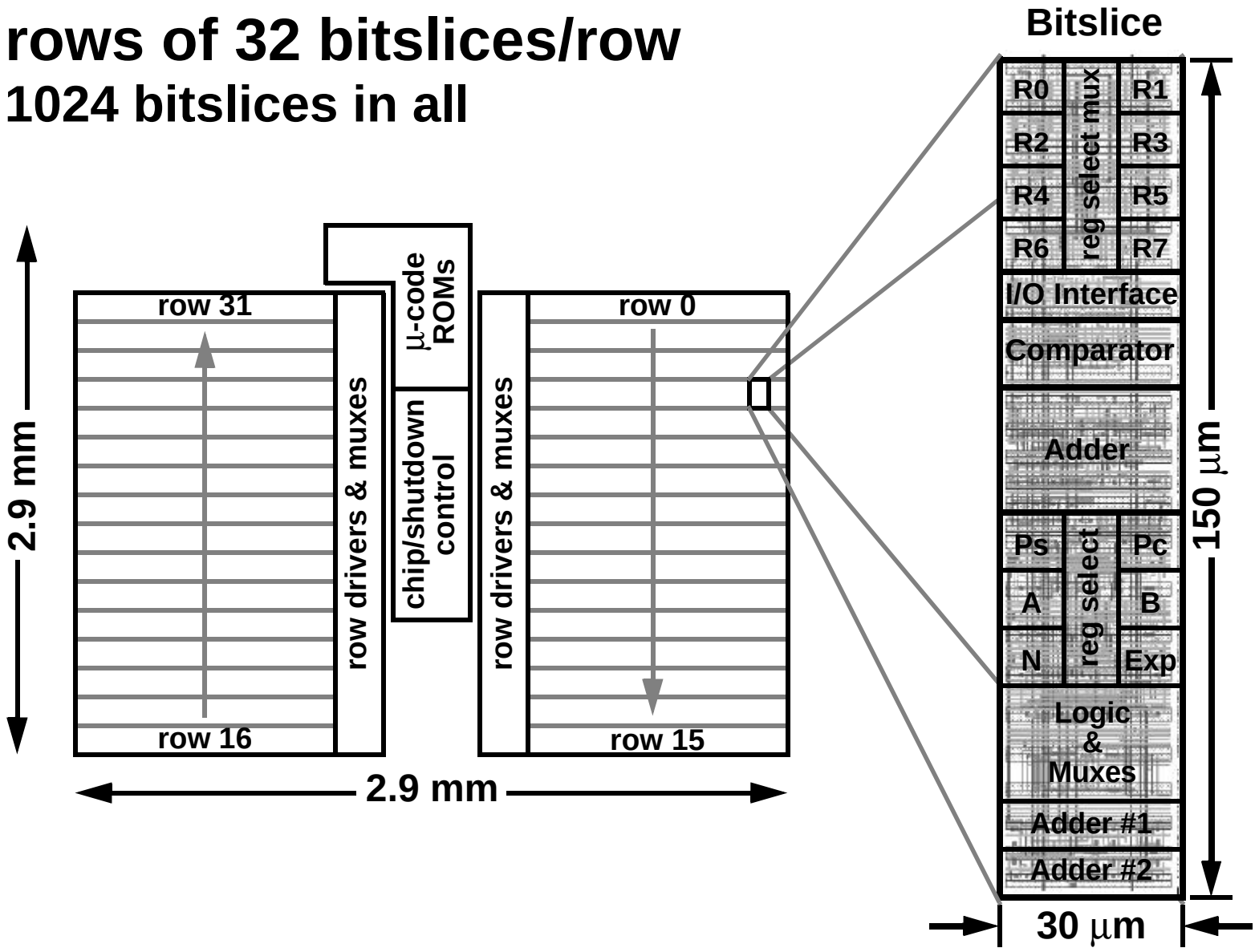


- All units shutdown in 32-bit increments

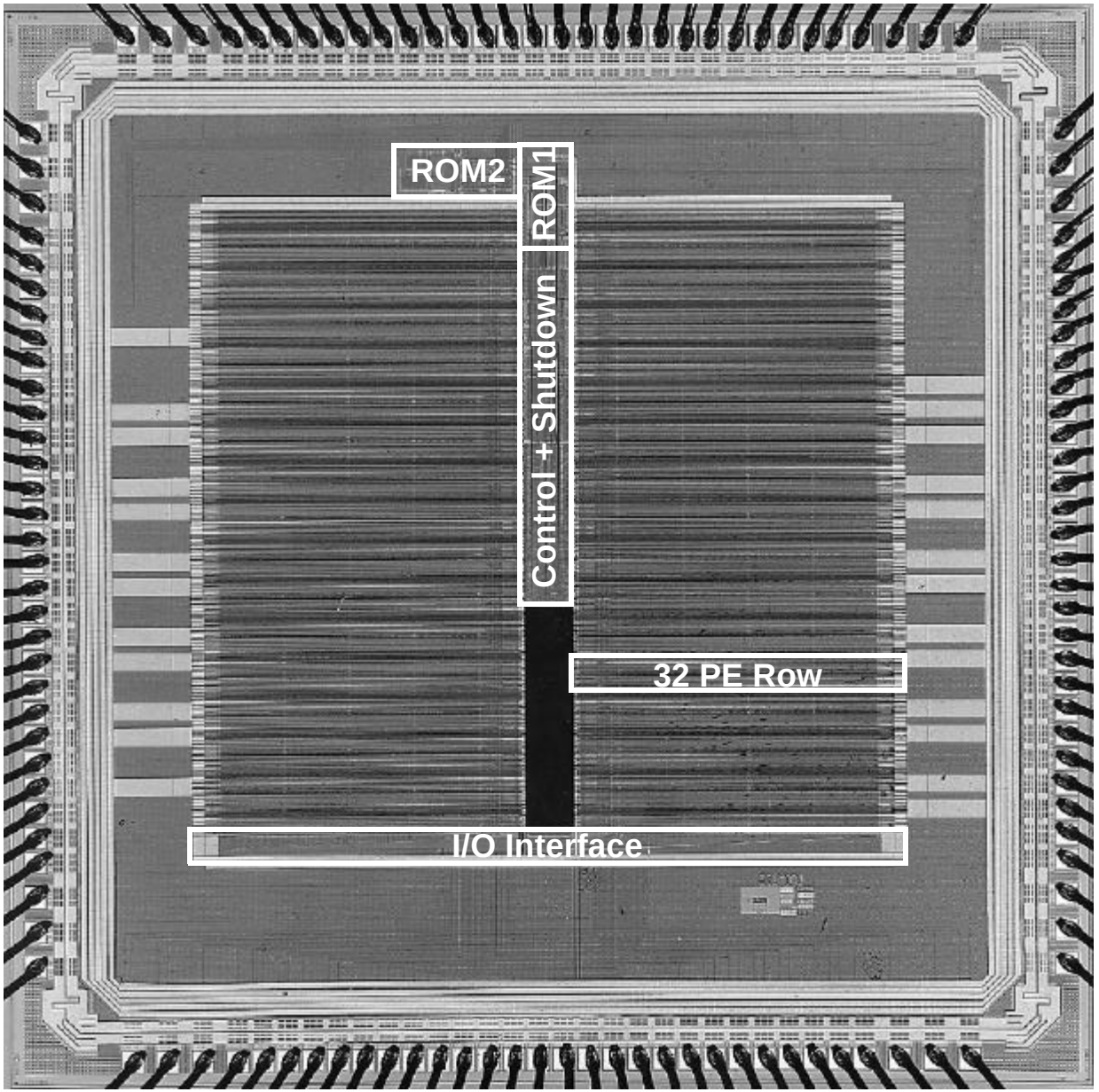


Ph

- **32 rows of 32 bitslices/row**
  - ⇒ **1024 bitslices in all**



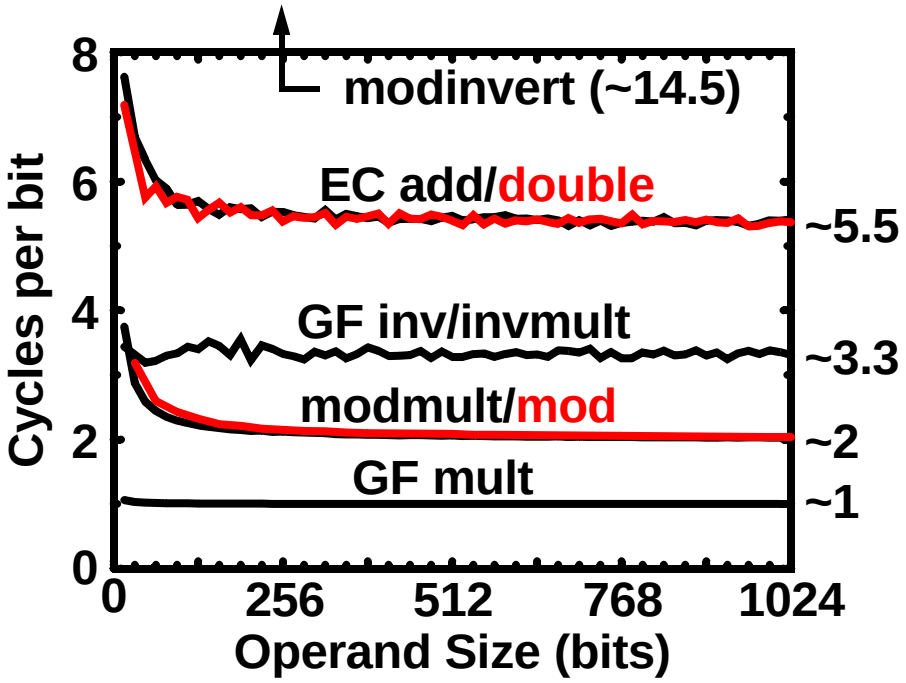
Reconfigurable Processor Fabrication

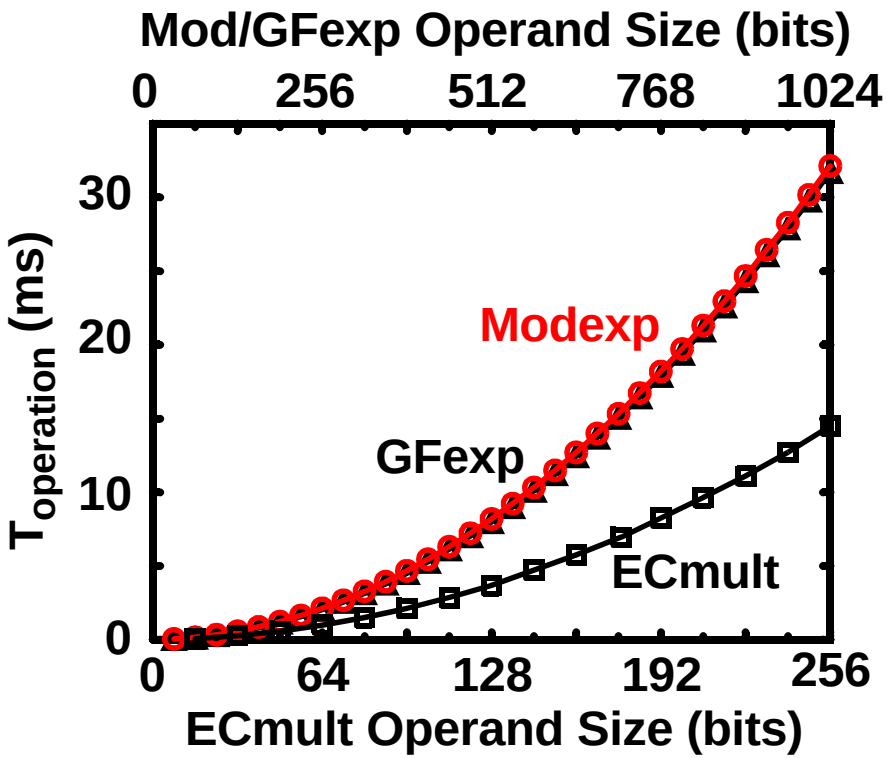


Process Specs

- 0.25 μm CMOS
- 1 Poly, 5 Metal
- VT = +/-0.55V
- 880k devices
- pad-limited (2.9 x 2.9 mm)

DSRCP Performance





- **Primitives performance points (@50 MHz):**

Modexp (IF/DL)	GFexp (DL)	ECmult (ECDL)
8.2/5.2 ms @ 512b 32.1/17 ms @ 1024b	8.0ms @ 512b 31.7ms @ 1024b	7.0ms @ 176b 14.5ms @ 256b

Comparison to Commercial Solutions

- **Modular Exponentiation**

Design	Power (mW)	Size (bits)	T_{modexp} (ms)	Efficiency (cyc/bit^2)	f_{clk} (MHz)
MPC180	600	1024	32	2.01	66
PCC-ISES	1000	2048 / 1024	6.02 / 1.45	0.07 / 0.07	50*
BC5820	"Low"	1024	1	0.1	100
DSRCP	< 75	1024 / 512	32.1 / 8.2	1.53 / 1.56	50
DSRCP (CRT)	< 45	1024 / 512	17 / 5.2	0.81 / 0.86	50

- **GF(2^n) Elliptic Curve Point Multiplication**

Design	Power (mW)	Size (bits)	$T_{ecmult-155}$ (ms)	Efficiency (cyc/bit^2)	f_{clk} (MHz)
MPC180E	600	155	11	30.21	66
DSRCP	10	155	5.4	11.24	50

Comparison to Academic Solutions

- **Modular Exponentiation:**

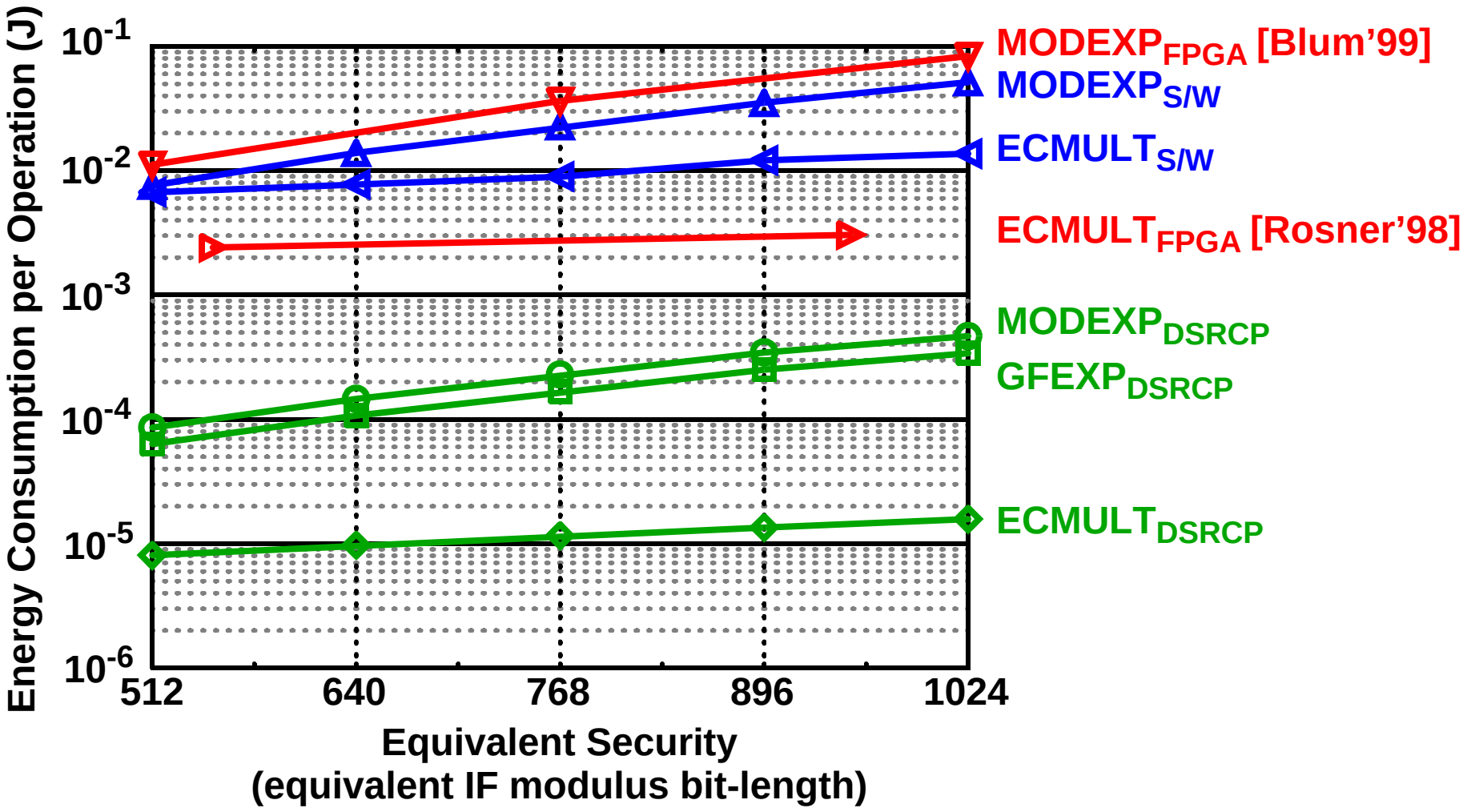
Design	Power Consumption (W)	Operand Size (bits)	Time per Operation (ms)	Cycles per Operation (cycles/bit^2)	Clock Rate (MHz)
Ishii	2	1024/512	100/25	3.81/3.81	40
Ivey	-	512	< 8	< 4.58	150
Orup	-	512	5	0.48	25
Chen	-	512	21	4.01	50
Yang	-	512	4.3	2.05	125
Guo	-	512	1.8	0.98	143
Leu	-	512	4.6	2.02	115
Royo	-	768	10.6	0.90	50
Satoh	0.33	1024	23	0.99	45
Vandemeulebroecke	0.50	1024	125	2.98	25
Shand	-	1024/512	6/0.85	0.23/0.13	40
Yuliang	-	1024	650	12.40	20
DSRCP	< 0.075	1024/512	32.1/8.2	~1.53/~1.56	50
DSRCP w/CRT	< 0.045	1024/512	17/5.2	~0.81/~0.86	50

Comparison to Academic Work

- **Elliptic Curve Point Multiplication:**

Design	Power Consumption (W)	Operand Size (bits)	Time per Operation (ms)	Cycles per Operation (Mcycles)	Clock Rate (MHz)
Agnew	-	155	8.1	13.49	40
Sutikno	-	155	21.6	13.49	15
DSRCP	~0.010	155	5.4	11.24	50

Comparison of Energy Efficiencies



DSRCP: ~100x-1000x more energy efficient

Conclusions

- **Domain-specific reconfigurability provides flexibility while minimizing overhead**
  - **⇒ Domain Specific Integrated Circuits (DSICs)**
- **Interconnect-centric architecture exploits locality to minimize interconnection overhead**
- **Public Key Cryptography DSIC provides full algorithm agility with 2-3 orders of magnitude better energy efficiency than GPP and FPGA**

Acknowledgements

- Fabrication and funding is provided by the National Semiconductor Corporation

- This work is also sponsored by the Defense Advanced Research Project Agency (DARPA) Power Aware Computing/Communication Program with the Air Force Materiel Command, USAF under agreement number F30602-00-2-0551