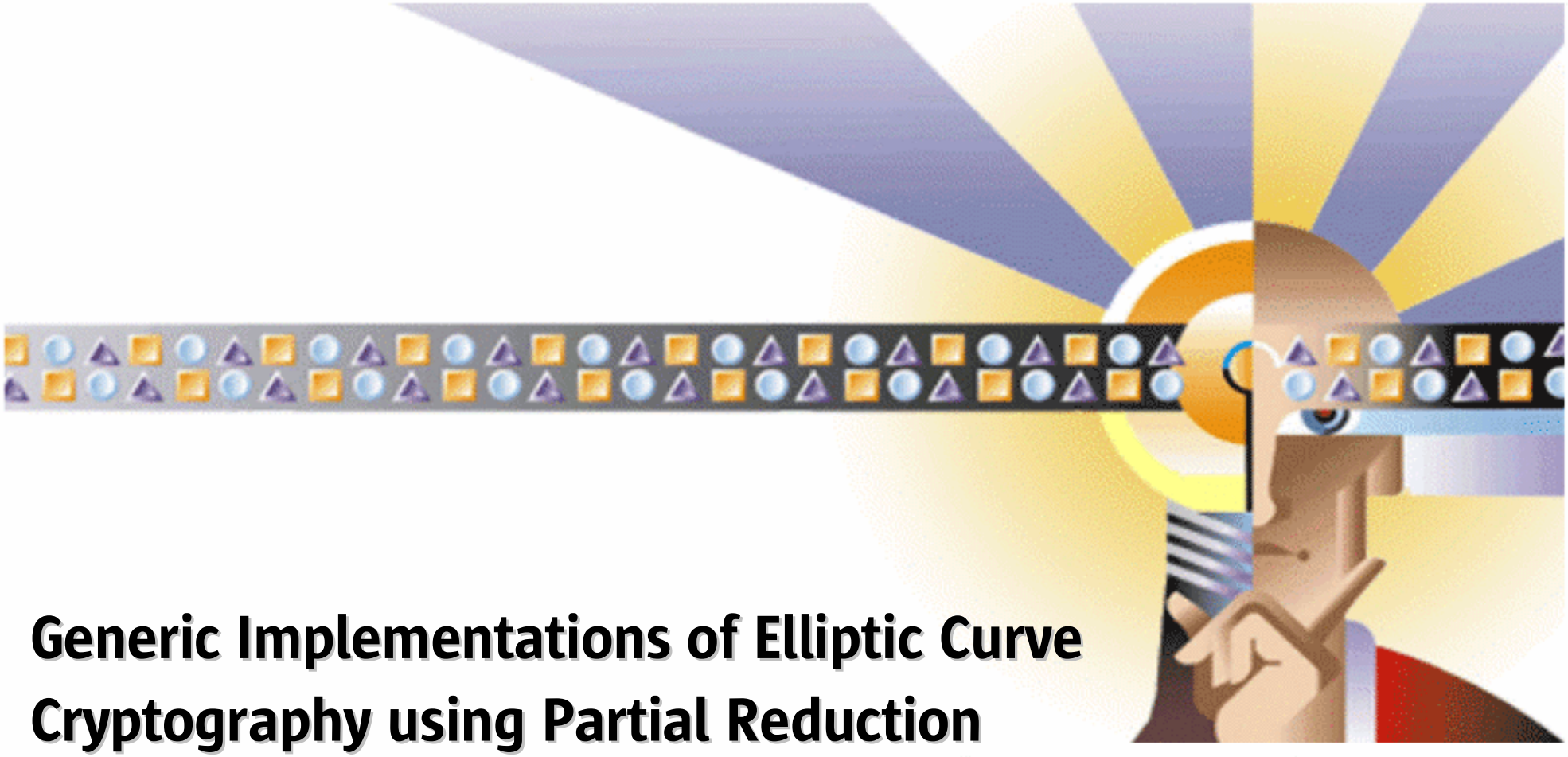


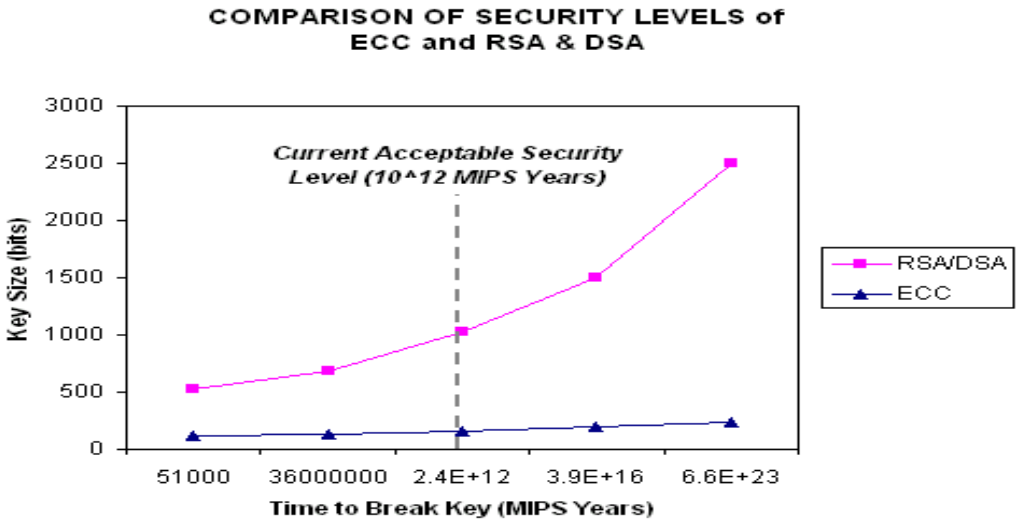
Generic Implementations of Elliptic Curve Cryptography using Partial Reduction

Nils Gura,
Hans Eberle,
Sheueling Chang Shantz

Sun Microsystems Laboratories

Sun microsystems
We make the net work.

Emerging Crypto Technologies

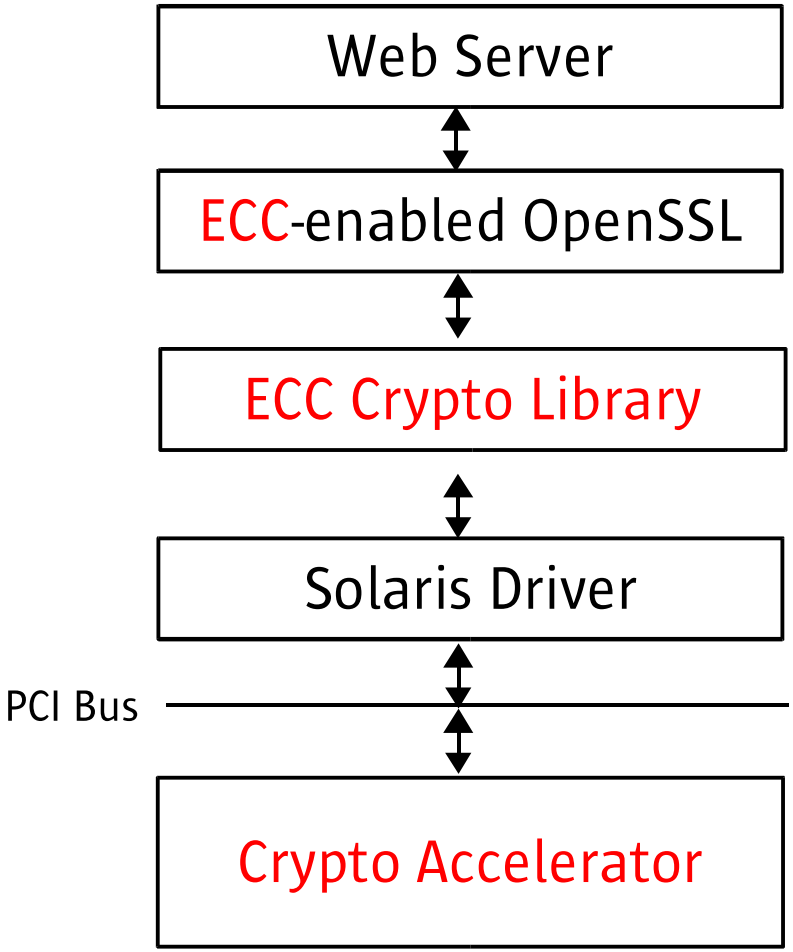


RSA/ECC Keysize Growth Ratio

DES	AES	RSA	ECC	RSA:ECC
64		512		
112		1024	163	7:1
	128	3072	283	11:1
	192	10240	409	25:1
	256	15360	571	27:1

- Elliptic curve crypto-system provides highest security strength per bit
- US government standardized ECC/AES in 2000/2001, plans to switch in 2005-2008 time frame
- ECC suitable for wireless hand-held devices
- Mobile applications drive market

System Overview



Complete ECC-enabled Hardware/Software stack

- Crypto library development
- Secure protocol integration
- Application support
- Hardware accelerator

Related Work

- Orlando/Paar 2000
  - digit-serial processing
  - highest reported performance
  - designed for specific curves
  - high reconfiguration overhead
- Goodman/Chandrakasan 2001
  - bit-serial processing
  - low power
  - designed for generic curves
  - low reconfiguration overhead

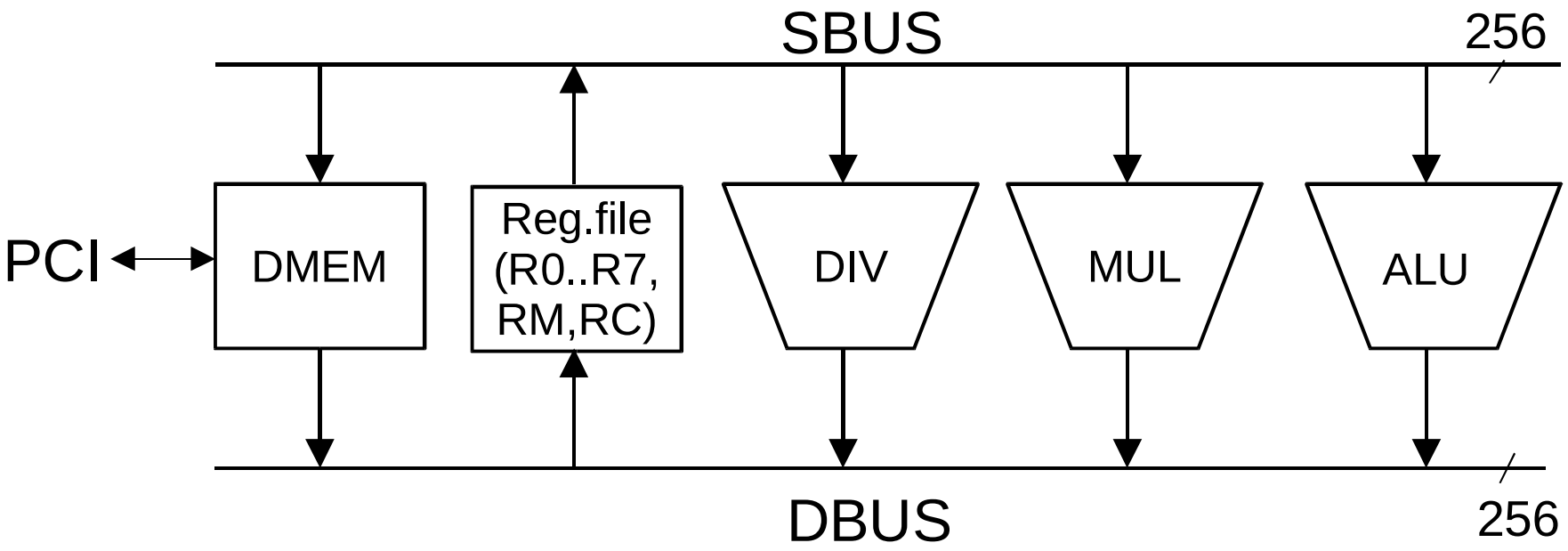
Web Server Acceleration

- Aggregation of secure connections with heterogeneous clients
- Fast implementation of named curves
  - NIST/SECG163, SECG193, NIST/SECG233
  - known field sizes and irreducible polynomials
- Support for generic curves
  - infrequently used curves
  - unknown curves
  - arbitrary field sizes and irreducible polynomials

Accelerator Characteristics

- Finite field arithmetic for GF(2^m), m≤255
- Arbitrary irreducible polynomials
- Microprogrammable architecture
- Overlapped and parallel instruction execution
- Bus-based data path
- FPGA prototype, 66 MHz clock
- 66 MHz/64-bit PCI interface

Accelerator Architecture

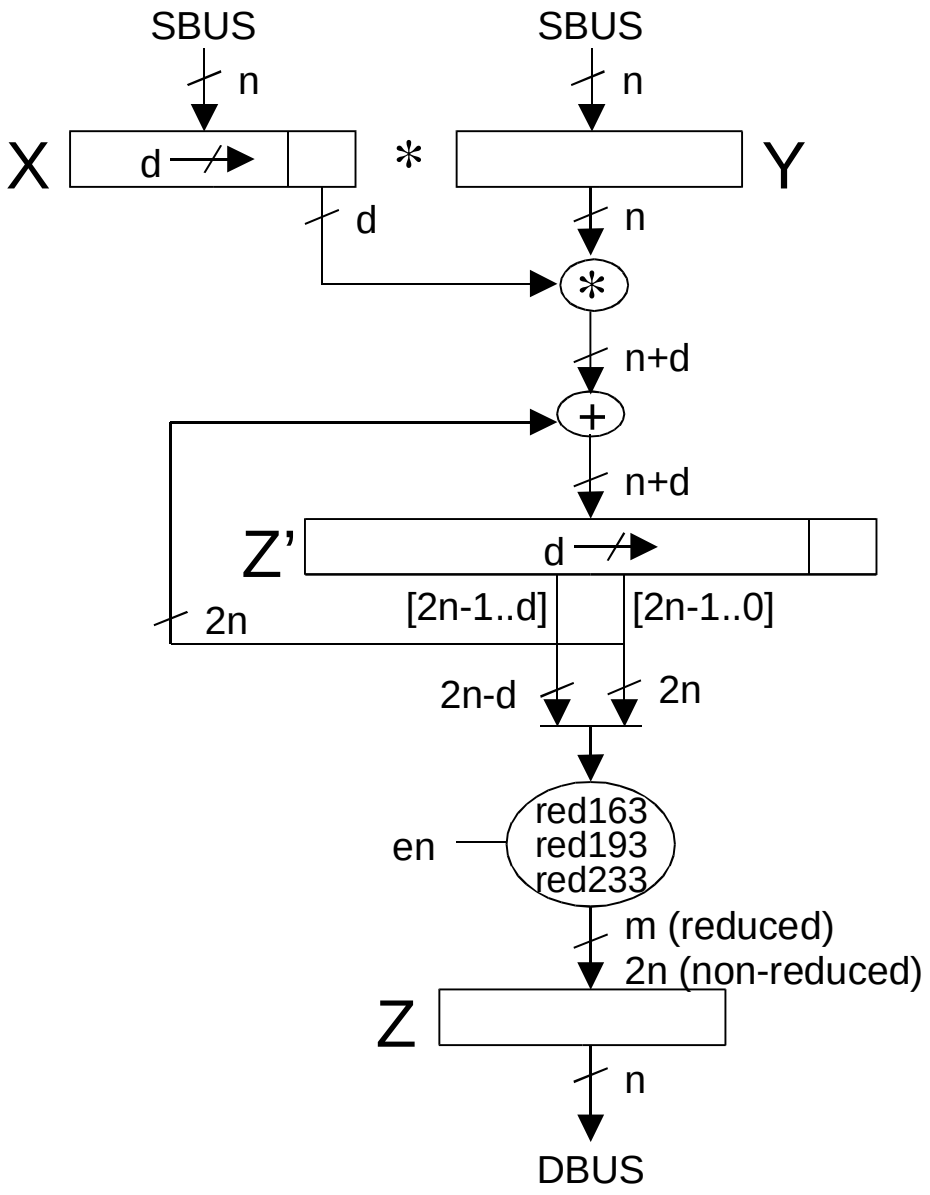


Instruction Set

Instruction		Name	Cycles
Memory Instructions			
LD	DMEM,RD	Load	3
ST	RS, DMEM	Store	3
Arithmetic Instructions			
DIV	RS0,RS1,RD	Divide	≤2m+4
MUL	RS0,RS1,RD	Multiply	7,8
MULNR	RS0,RS1,RD	Multiply w/o Reduction	8
ADD	RS0,RS1,RD	Add	3
SQR	RS,RD	Square	3
SL	RS,RD	Shift Left	3
Control Instructions			
BMZ	ADDR	Branch if MSB zero	2
BEQ	ADDR	Branch if equal	4
JMP	ADDR	Jump	2
END		End	

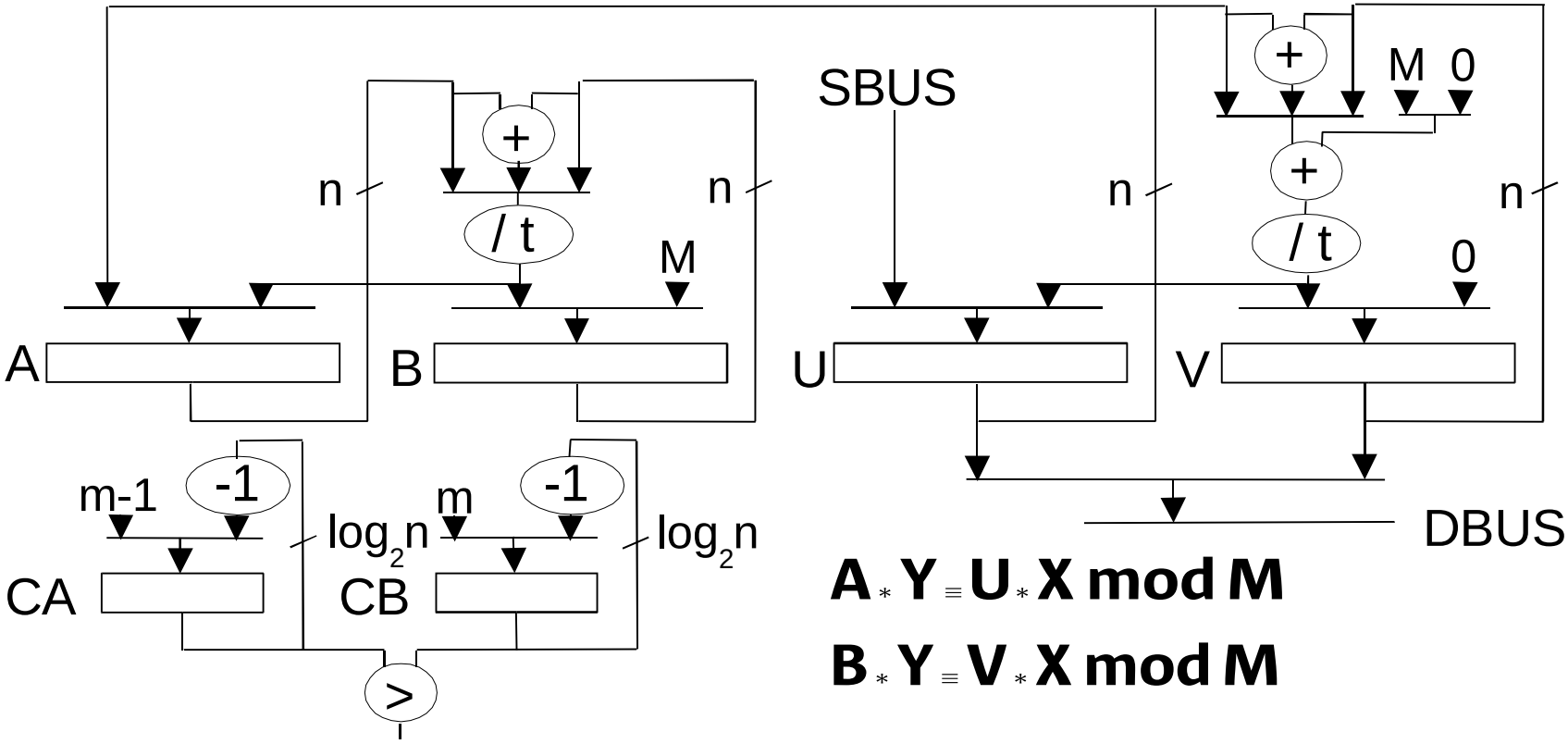
Multiplier

- Digit-serial multiplier (n=256, d=64)
- Hard-wired reduction for GF(2^{163}), GF(2^{193}), GF(2^{233})
- Unreduced product for partial reduction
- Cycle counts:
  - m < 192: 7 cycles
  - m ≥ 192: 8 cycles



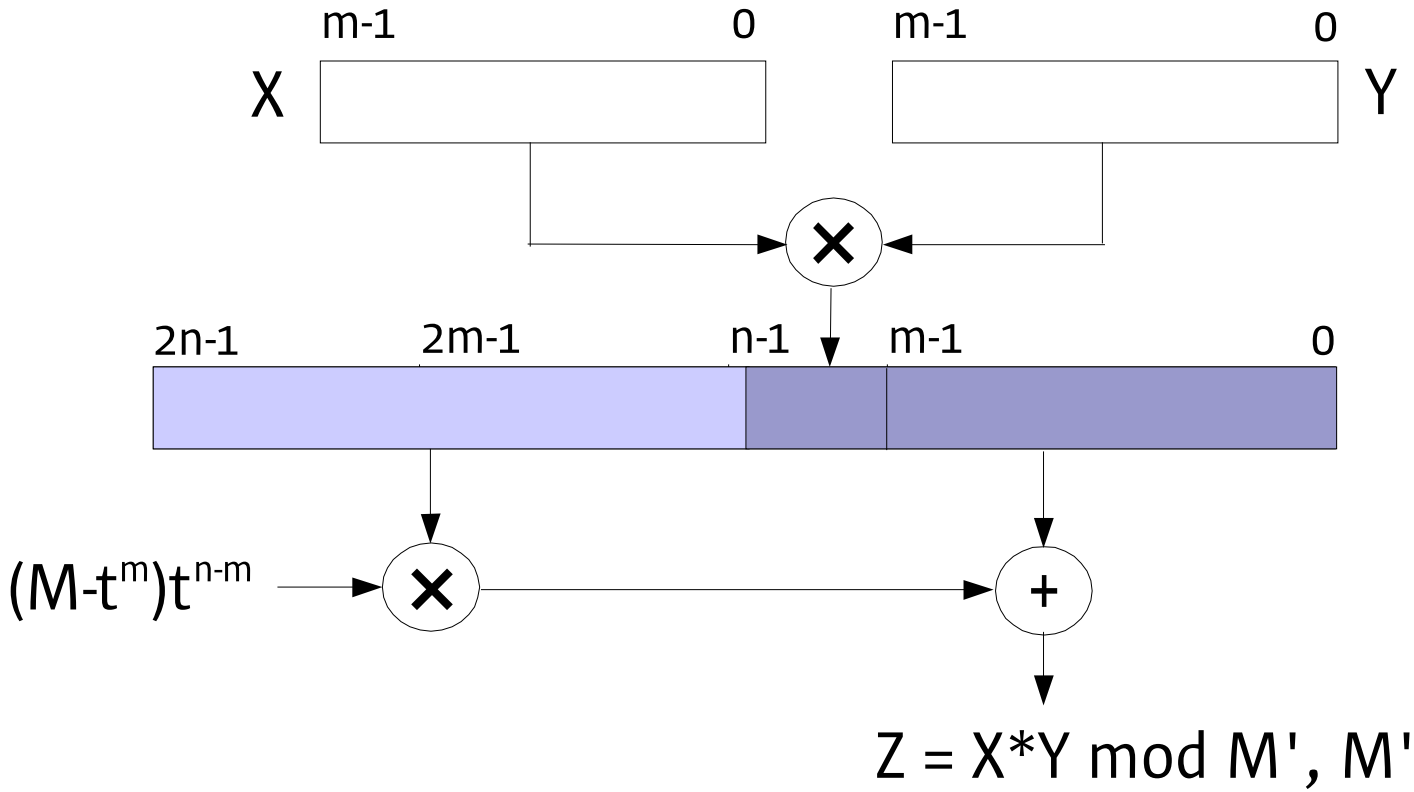
Divider

- Computes Y/X mod M for arbitrary irreducible polynomials M
- Faster than soft-coded inversion algorithms

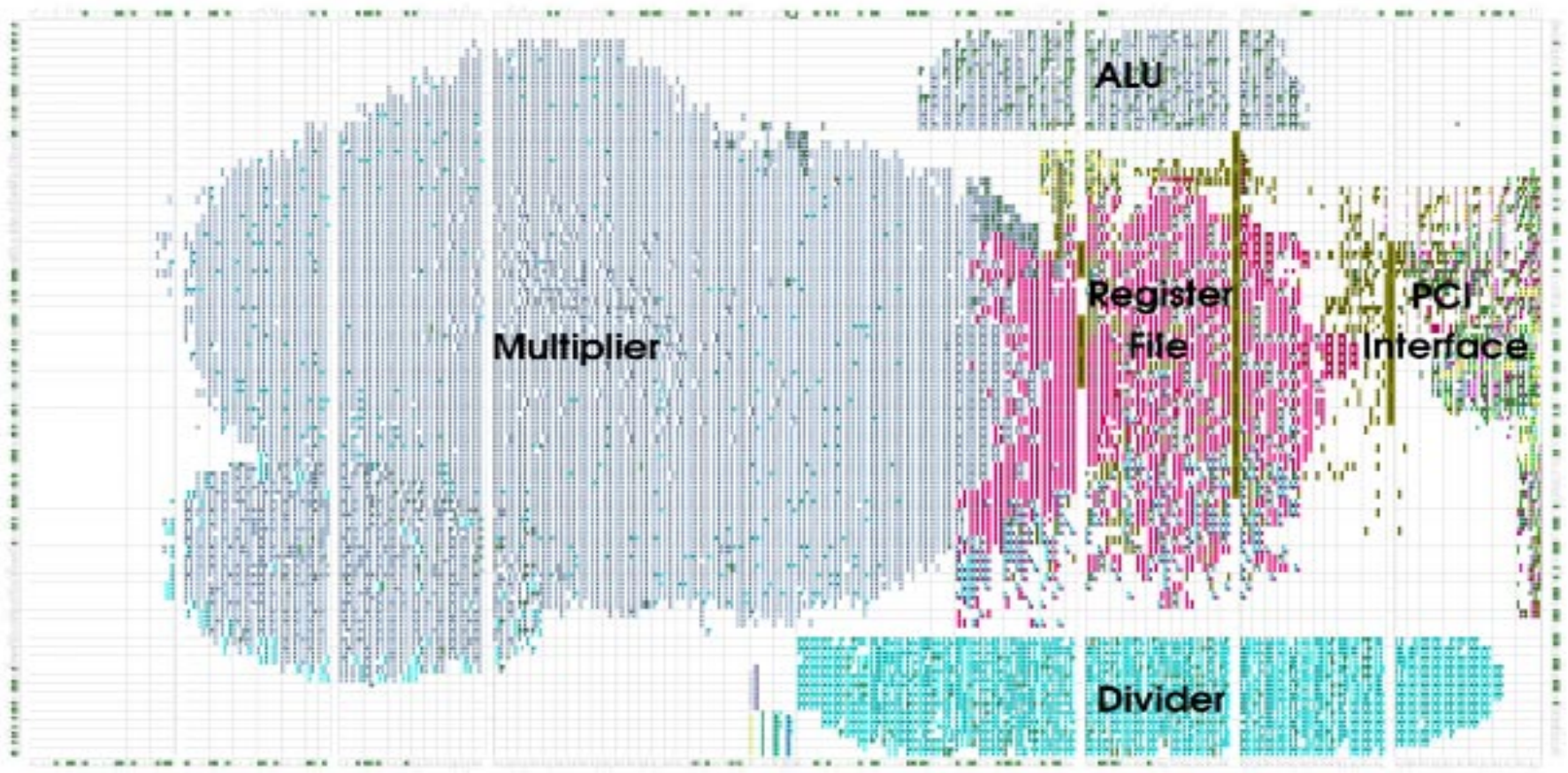


Partial Reduction

- MUL and SQR require *mod M* operation
- Partial reduction operates on n-bit operands independent of field degree m



Accelerator Floorplan



Technology: Xilinx XCV2000E FPGA
Size: 20068 LUTs, 6321 FFs
Clock: 66 MHz

Performance

	Hardware op/s	Software op/s	Speedup
Named Curves			
GF(2^{163})	6987	322	21.7
GF(2^{233})	4438	223	19.9
Generic Curves (full)			
GF(2^{163})	644	322	2.0
GF(2^{233})	451	223	2.0
Generic Curves (part.)			
GF(2^{163})	1075	50	21.5
GF(2^{233})	757	35	21.6

Conclusions

- Web servers demand support for multiple named curves and arbitrary generic curves
- Partial reduction algorithm simplifies modular arithmetic on generic curves
- Generic reduction is costly
- High mul/div ratio favors projective coordinate representation

Web Resources

- Sun Labs Website
  - http://www.research.sun.com
  - http://www.experimentalstuff.com
- Next Generation Crypto Project
  - http://research.sun.com/projects/crypto
- OpenSSL
  - http://www.openssl.org