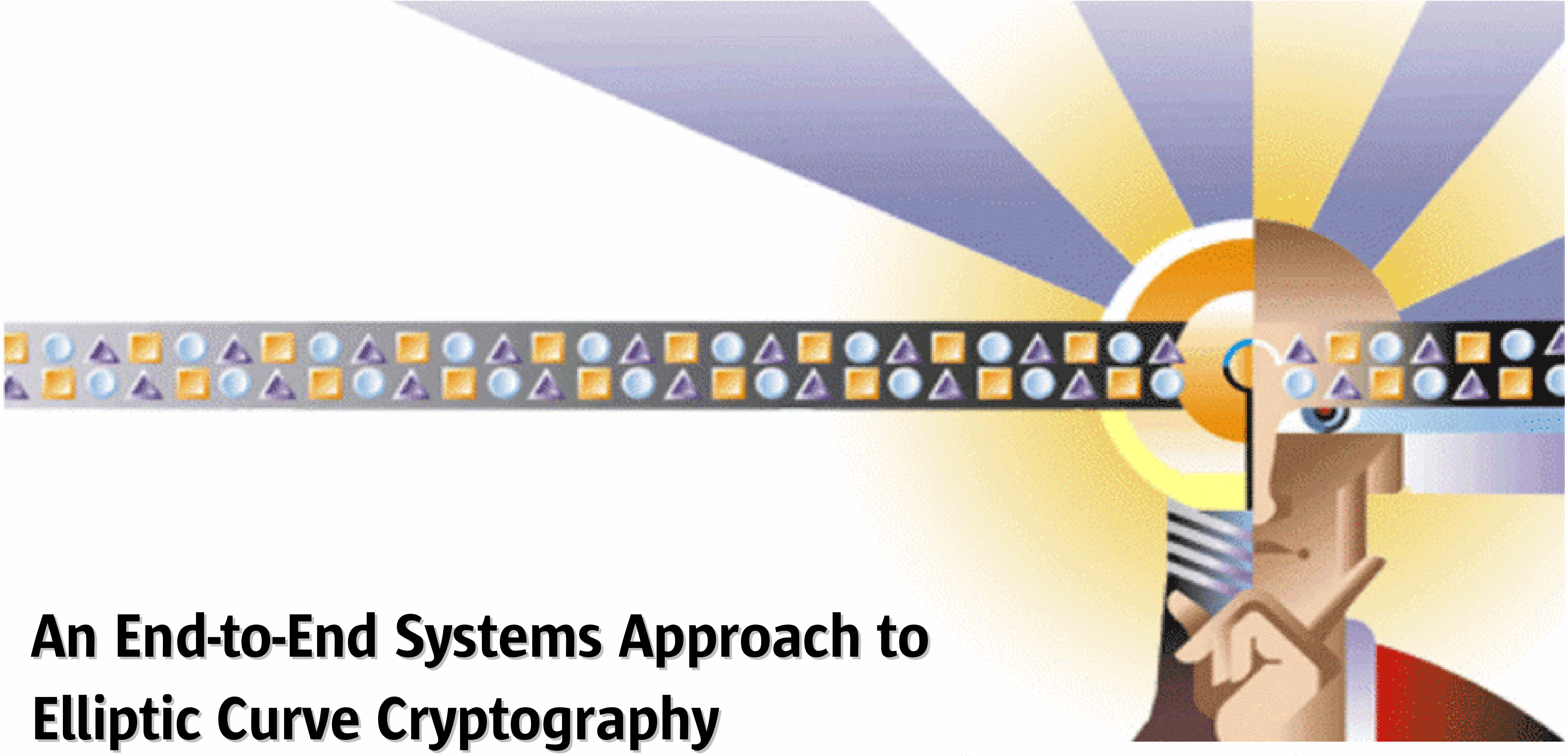


An End-to-End Systems Approach to Elliptic Curve Cryptography

Nils Gura,
Sheueling Chang Shantz, Hans Eberle,
Sumit Gupta, Vipul Gupta,
Daniel Finchelstein, Edouard Goupy,
Douglas Stebila

Sun Microsystems Laboratories

Sun microsystems
We make the net work.

ECC for Commercial Applications

- Confidence in the security of ECC
- Integrated into secure protocols (SSL, IPsec)
- Conformance with standards, e.g. IEEE P1363, ANSI X9.62, X9.63
- Small, cost-efficient, low-power implementations on client devices
- High-performance server-side implementations, >5000 ops/s for ECC-163
- Ability to process a range of curves on the server side

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

Typical Assumptions

- Squarings are cheap
- Register size == key size
- Reduction can be hardwired
- Different curves can be handled with reconfigurable hardware

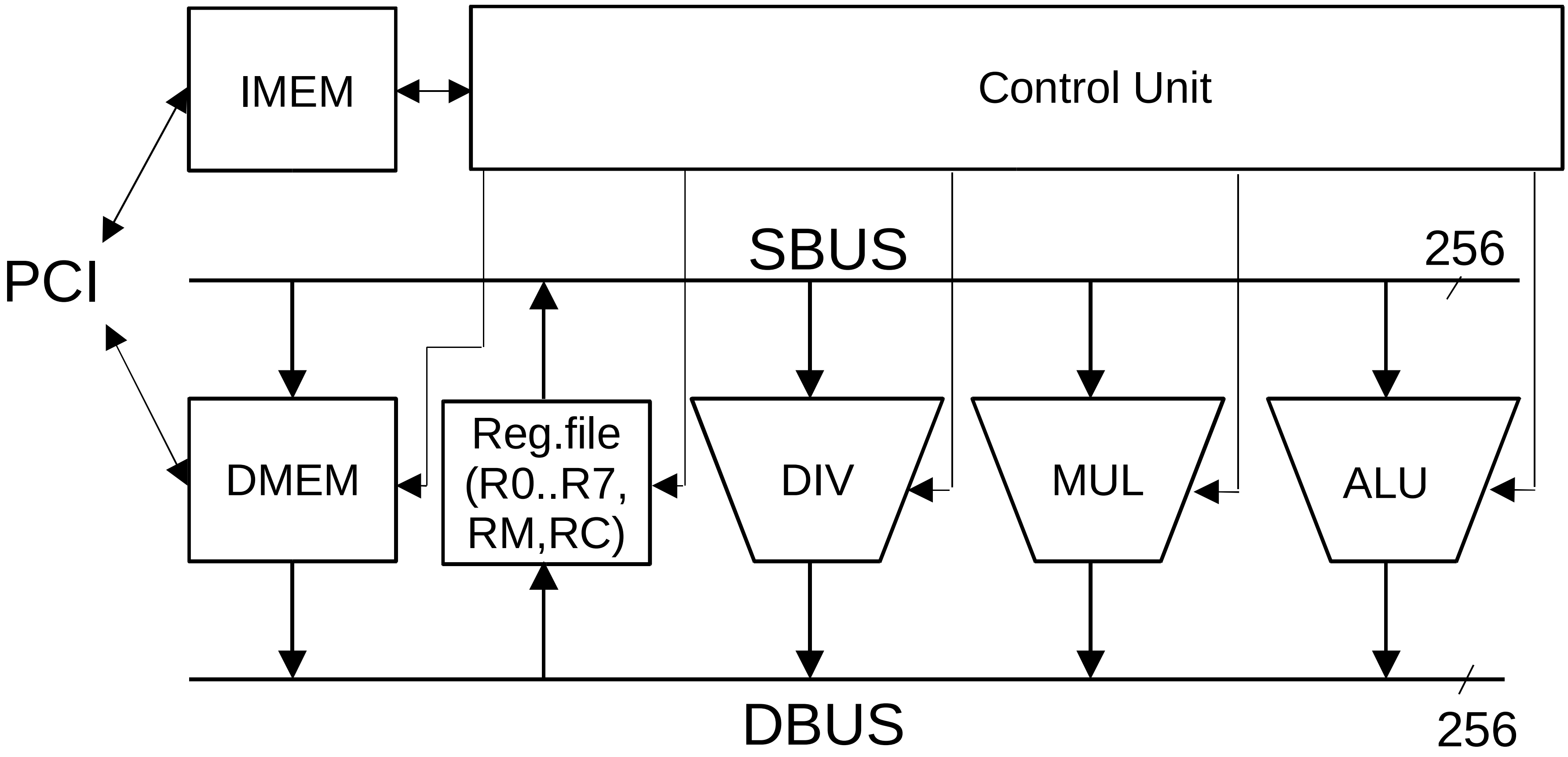
Challenges

- Multiple named curves
  - listed in standards
  - known irreducible polynomials
- Generic curves
  - not known at implementation time
  - infrequently used
- Various field sizes
- High performance
- System integration

Accelerator Characteristics

- Finite field arithmetic for $GF(2^m)$, $m \leq 255$
- Arbitrary irreducible polynomials
- Microprogrammable architecture
- Overlapped and parallel instruction execution
- 66 MHz clock
- 66 Mhz/64-bit PCI interface

Accelerator Architecture

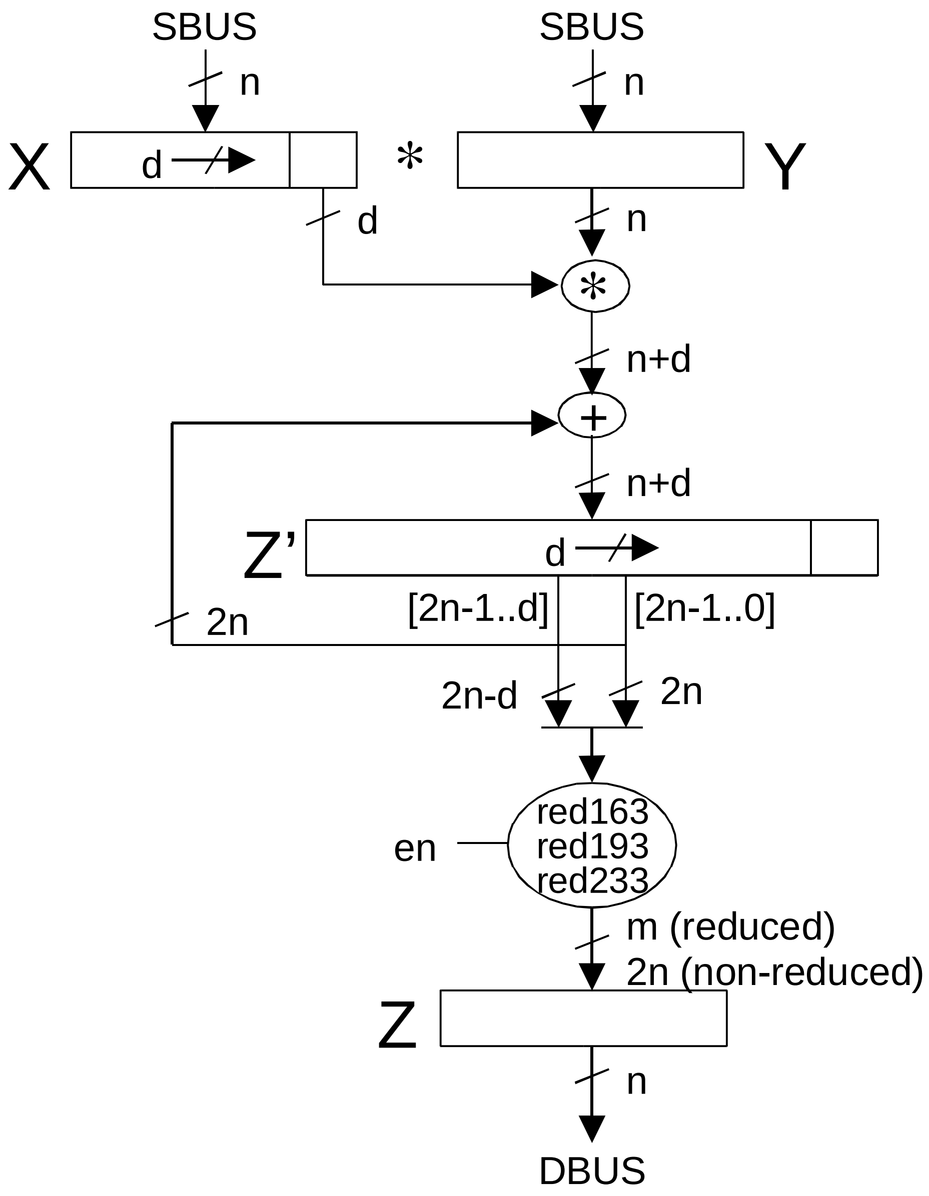


Instruction Set

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	8 (7)
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	

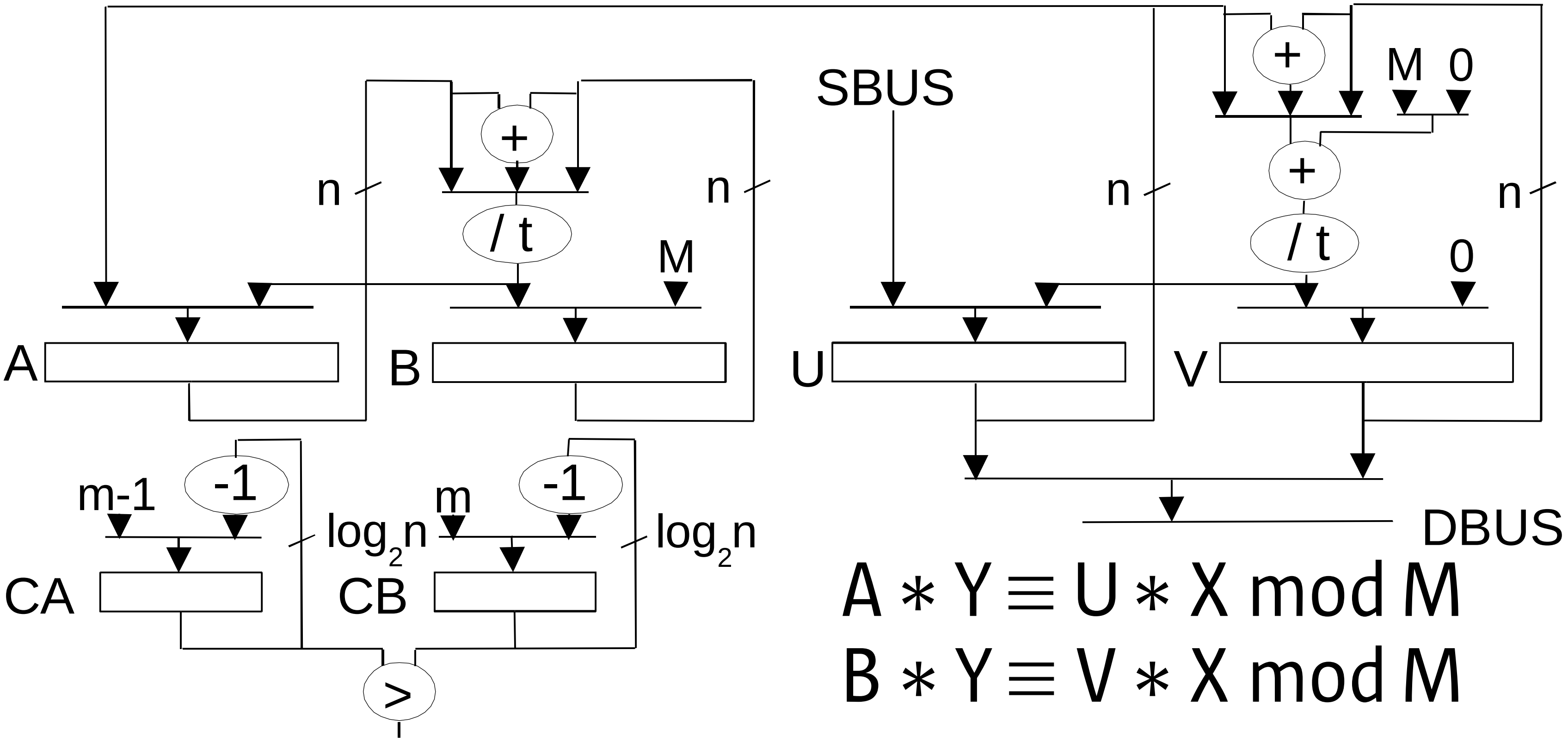
Multiplier

- Register sizes
  X,Y,Z: n=256
  Z': 2n=512
- Digit size d=64
- $\lceil m/d \rceil + 1$ cycles
- Hardwired reduction for $GF(2^{163})$, $GF(2^{193})$, $GF(2^{233})$



Divider

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

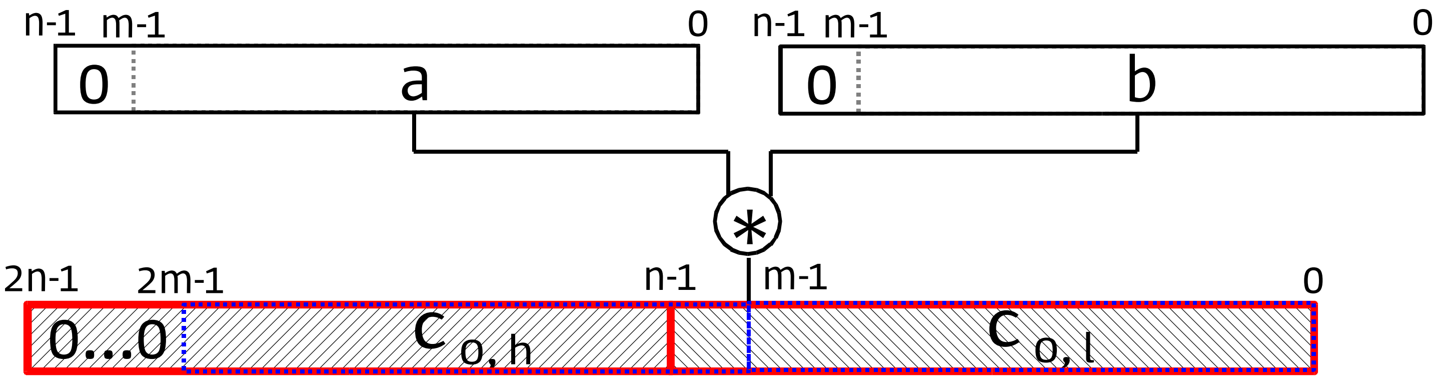


$$A * Y \equiv U * X \bmod M$$

$$B * Y \equiv V * X \bmod M$$

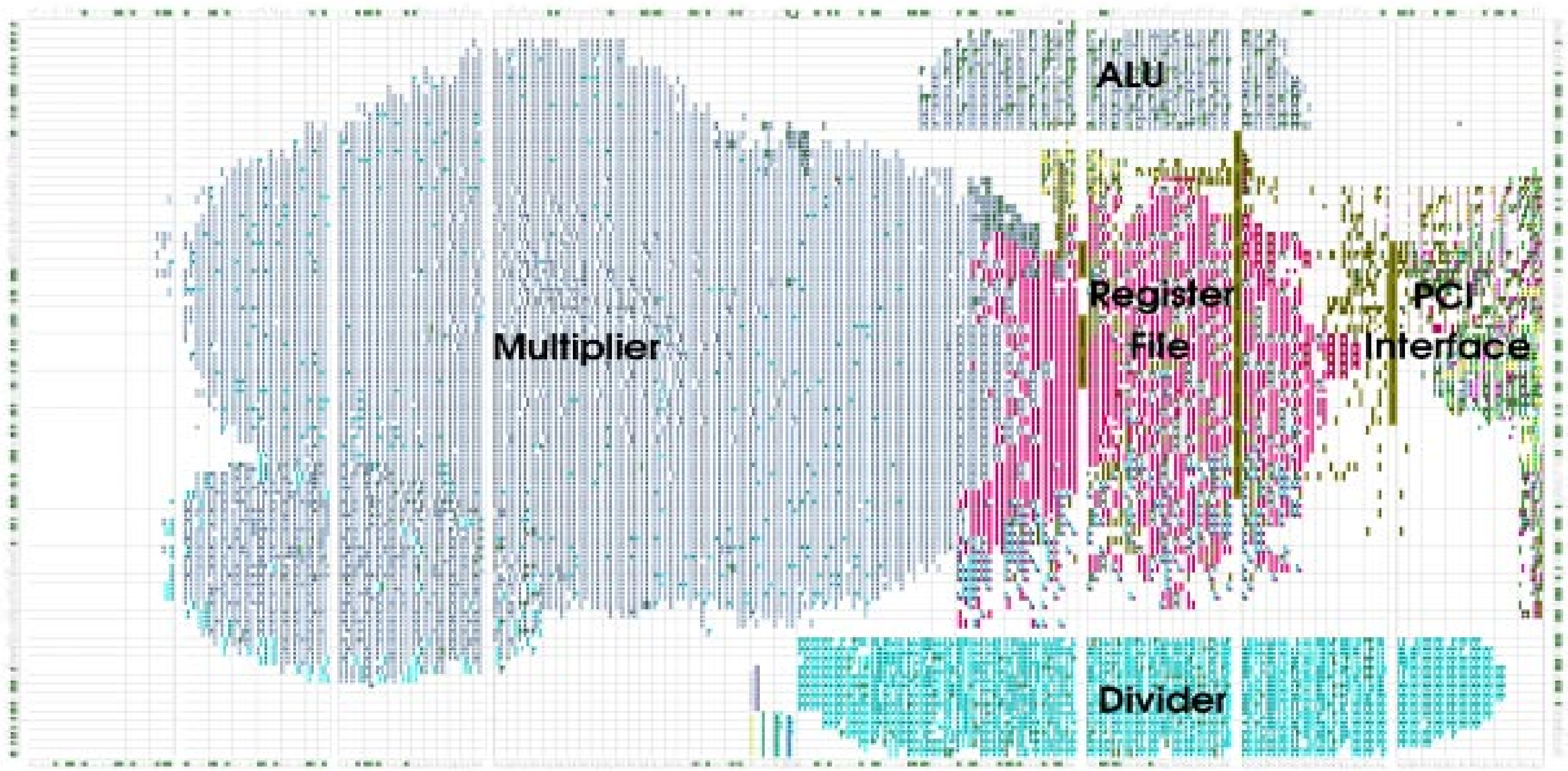
Generic Curves

- Register size > key size



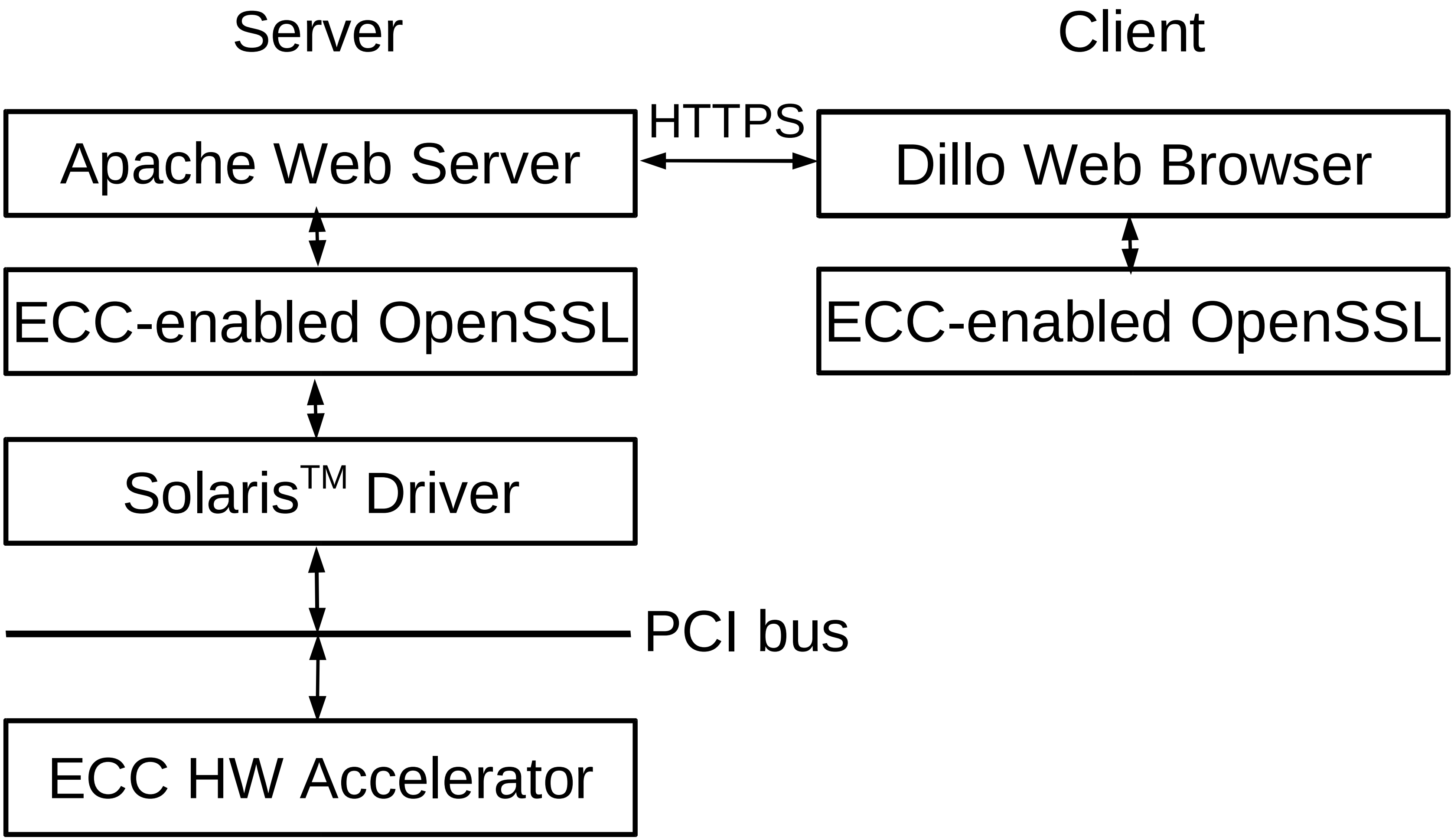
- Single multiplication requires 4 MULNR and 1 ADD instruction including reduction
- Squarings as expensive as multiplications
- Soft-coded inversion algorithms become expensive

Accelerator Floorplan



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

System Overview



Performance

ops/s	Hardware	Software	Speedup
Named Curves			
GF(2^{163})	6987	322	21.7
GF(2^{233})	4438	223	19.9
Generic Curves			
GF(2^{163})	644	322	2.0
GF(2^{233})	451	223	2.0
ECDH			
GF(2^{163})	3813	304	12.5
ECDSA (sign)			
GF(2^{163})	1576	292	5.4
ECDSA (verify)			
GF(2^{163})	1224	151	8.1

Conclusions

- Designed and built unified accelerator architecture for both named and generic curves
- Support for multiple curves without reconfiguration
- Reduction is the costliest operation for generic curves
- High mul/div ratio favors projective coordinate representation
- Performance evaluation on the system level