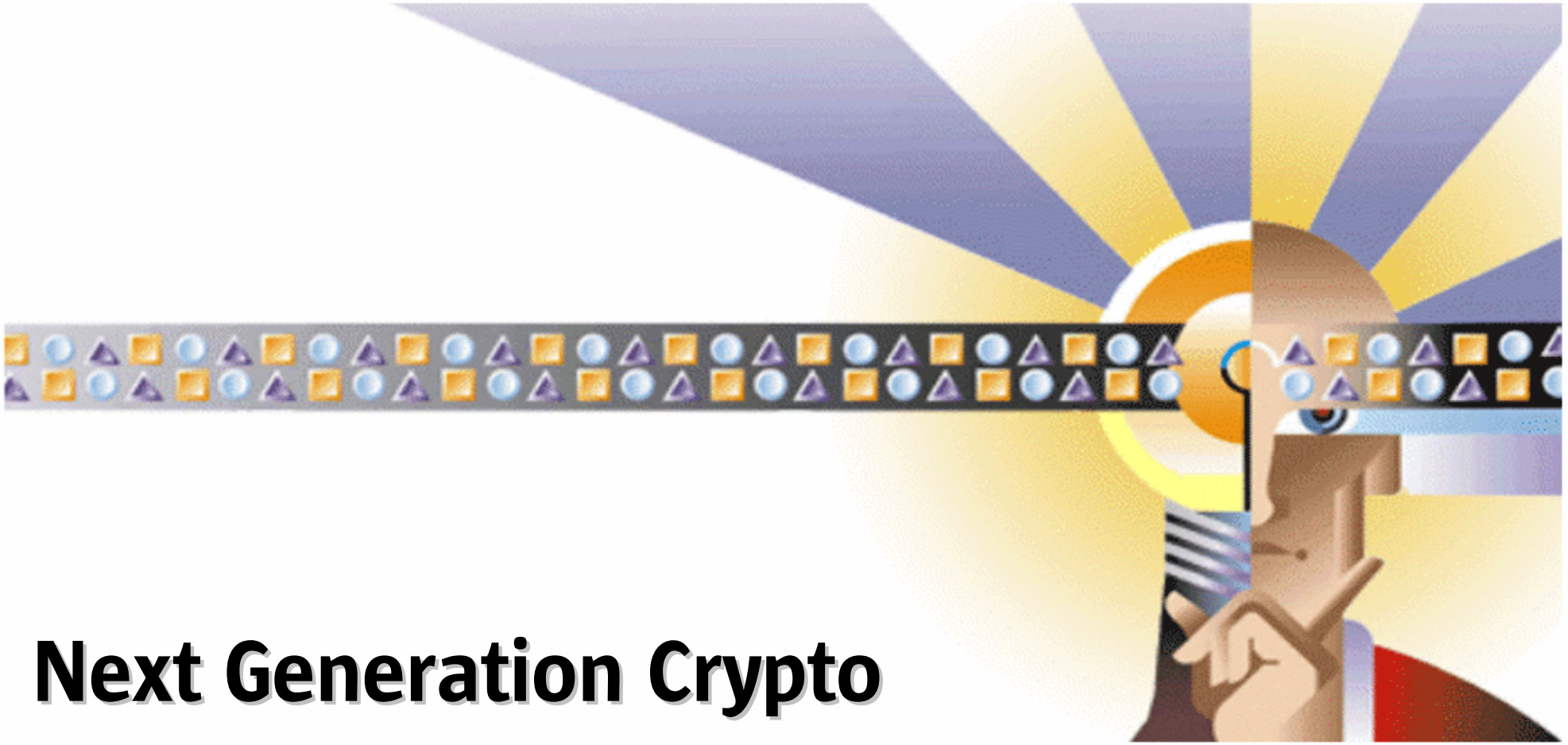


Next Generation Crypto

Sheueling Chang Shantz,
Hans Eberle, Nils Gura,
Vipul Gupta

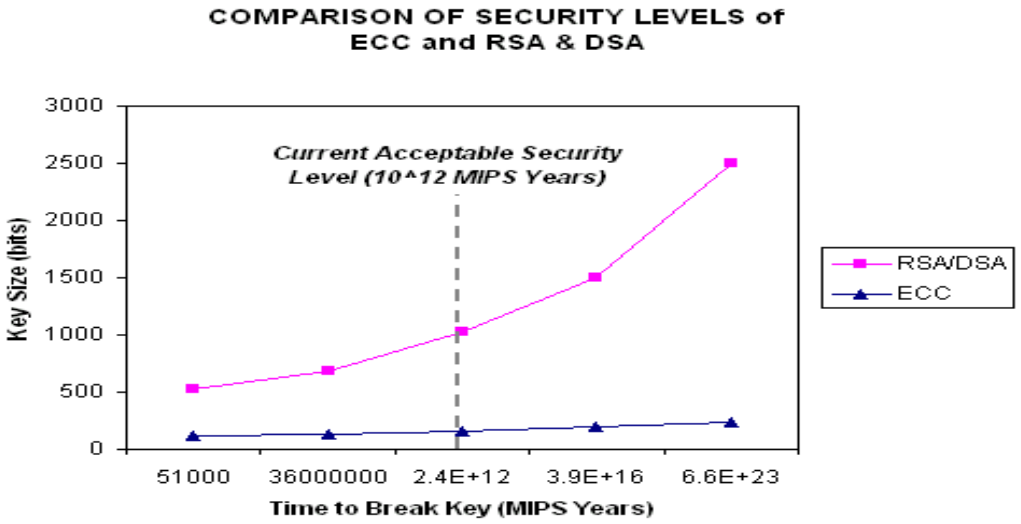
Sun Laboratories

Sun microsystems
We make the net work.

Security on the Web Today

- E-commerce secured by https
- Prevalent cryptographic technologies RSA/DES
- Prohibitively large RSA keys (AES-256 matches RSA-15,360)
- RSA signature generation slow on small devices
- Emerging cryptographic technologies ECC/AES

Emerging Crypto Technologies

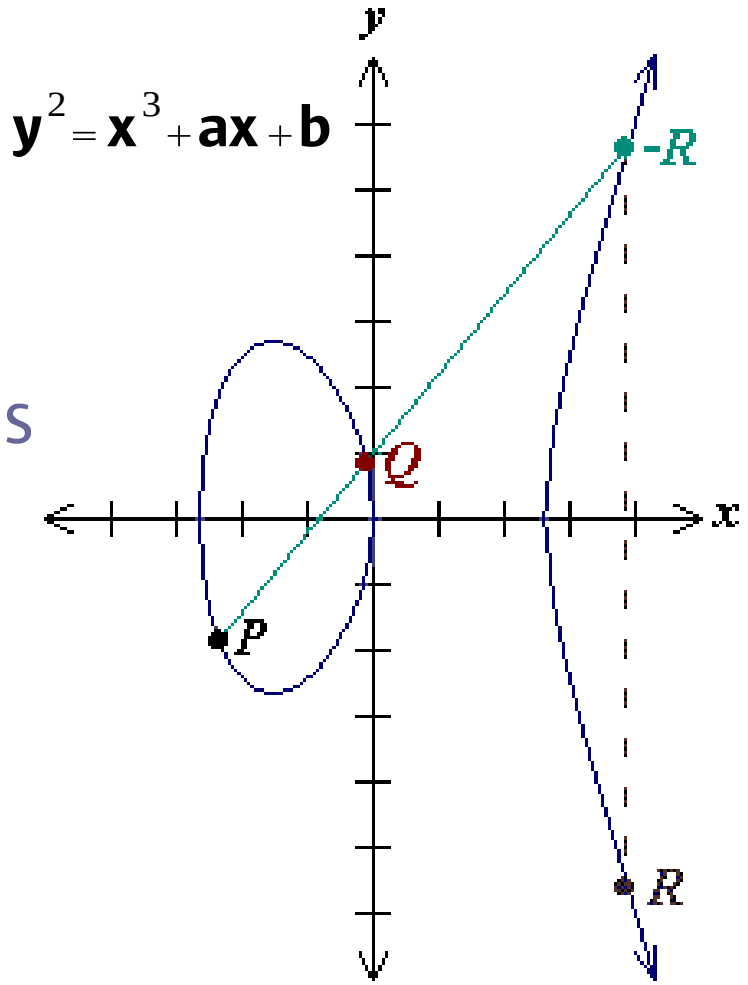


DES	AES	RSA	ECC	RSA:ECC
64		512		
112		1024		
	128	3072	283	11:1
	192	10240	409	25:1
	256	15360	571	27:1

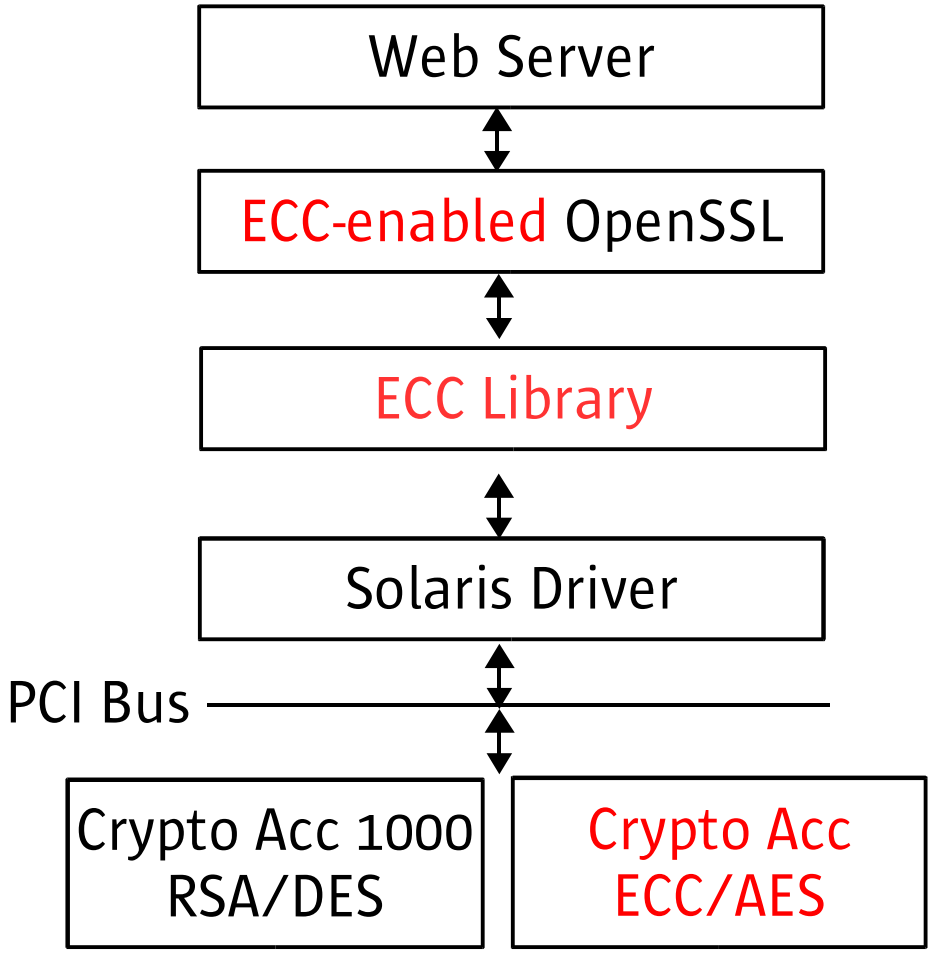
- Elliptic curve crypto-system provides highest security strength per bit
- US government standardized ECC/AES in 2000/2001, plans to switch in 2005-2008 time frame
- ECC suitable for wireless hand-held devices
- Mobile applications drive market

Elliptic Curve Public Key System

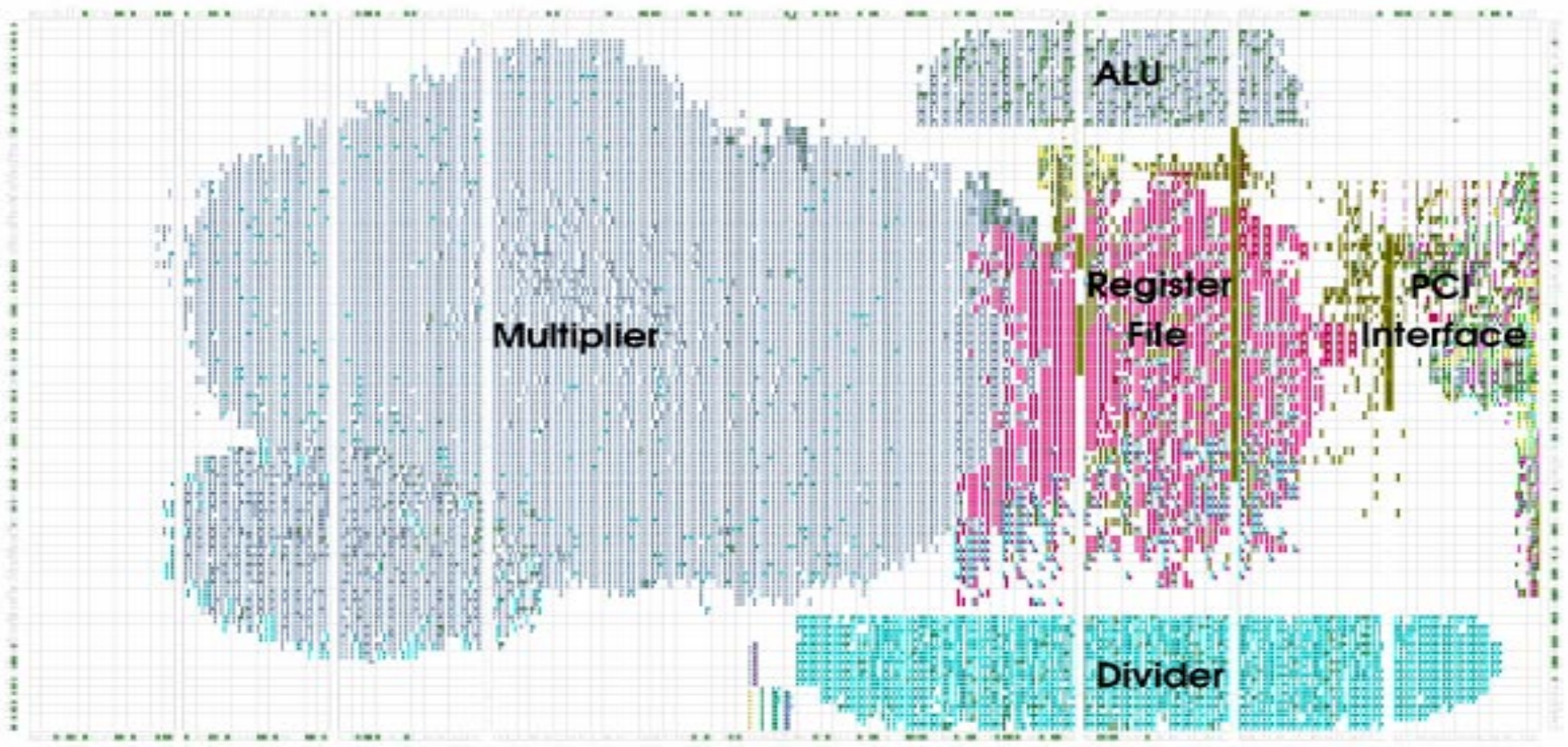
- ECC operation:
  point multiplication
  R (x,y) = k P (x,y)
- Repeated
  point additions and doublings
  9P = P + 2(2(2P)))
- Binary polynomial fields
- Prime fields
- ECC 163-bit == RSA 1024-bit



Next Generation Crypto Project



ECC Accelerator



256-bit MUL, DIV, ADD, SQR
66 MHz clock
64 bit / 66 MHz PCI

Performance:
ECC-163: 6987 ops/s, 21.7x (UltraSPARC III/
ECC-233: 4438 ops/s, 19.9x 900 MHz)