certicom
securing innovation

protect your content, applications and devices

with government-approved security

certicom
securing innovation

Benefits of ECC on Server Performance

Source and Methodology

- Study of ECC in SSL presented by Sun*
- Based on Badia's survey of Amazon, Datek, Fidelity, Etrade, Merrill Lynch & Wells Fargo
  - Two models for connection reuse
    - Shopping cart model (66% reuse)
    - financial institutions (87.5% reuse)
  - Requested page size range: 10KB to 70KB with 30KB mean
- Compares two types of cipher suites
  - RSA with AES at two strengths
  - ECDSA, ECDH with AES at corresponding strengths
- Public key operations in SSL

	RSA	ECDSA, ECDH	Reused Connection
Client	RSAverify + RSAencrypt	ECDSAverify + ECDH	None
Server	RSAdecrypt	ECDH	None

*Source: Sun Microsystems presentation to Network and Distributed System Security Symposium, 2004, Gupta, Stebila, Chang, et al. found at http://research.sun.com/projects/crypto/NDSS2004-presentation.pdf

Benchmark Performance

Crypto Operations Benchmarks

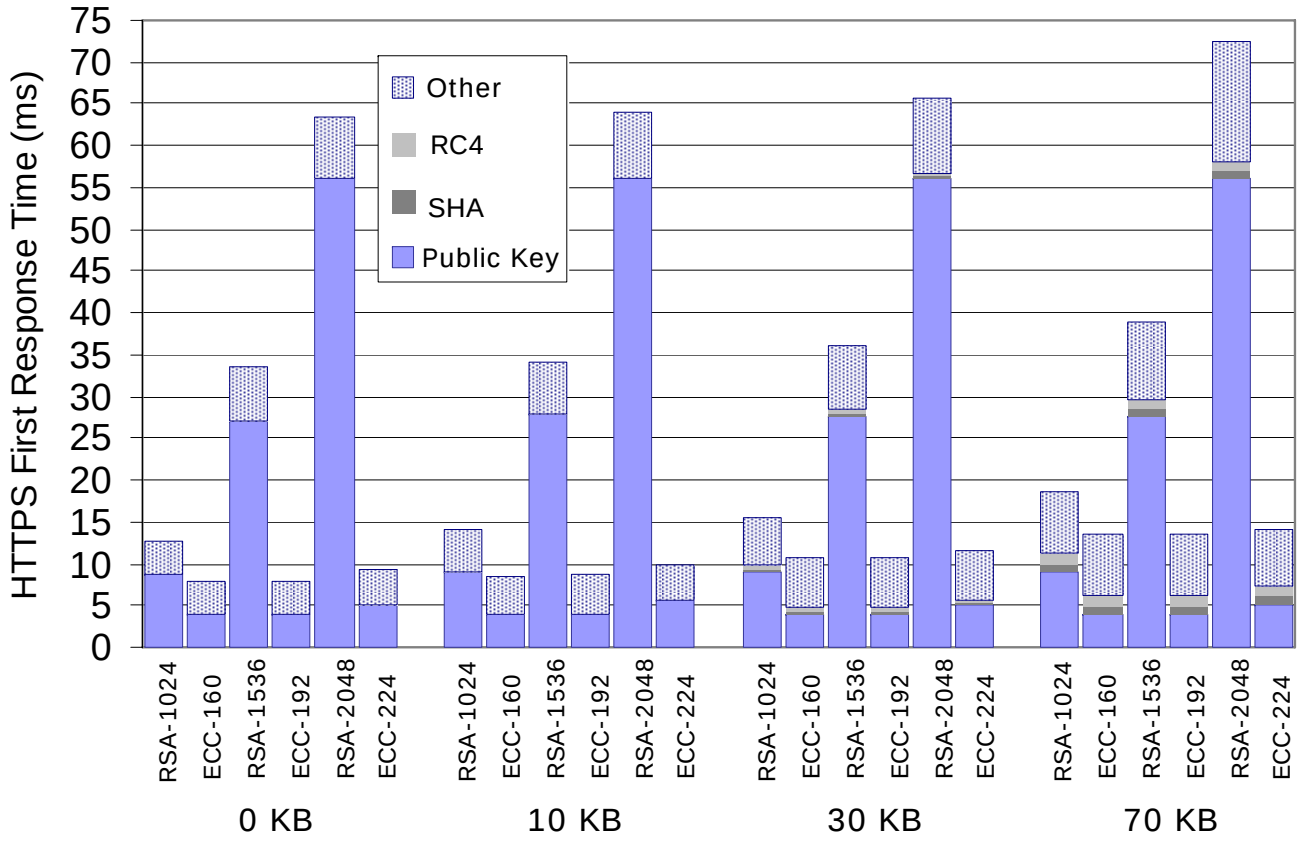
	ECC-160	RSA-1024	ECC-224	RSA-2048
Time (ms)	3.69	8.75	5.12	56.18
Operations/Sec	271.3	114.3	195.5	17.8
Perf. Ratio	2.4 : 1		11 : 1	
Key-size Ratio	1 : 6.4		1 : 9.1	

- $RSA_{private}$ operation versus ECDH operation
- ECC curves: secp160r1 and secp224r1
- ECC's performance advantage increases as security strength increases, and ECC-224 (the equivalent ECC key size to RSA 2048) is even faster than RSA 1024

Chart source: Sun Microsystems presentation to Network and Distributed System Security Symposium, 2004, Gupta, Stebila, Chang, et al. found at http://research.sun.com/projects/crypto/NDSS2004-presentation.pdf

certicom

Relative Computation Costs



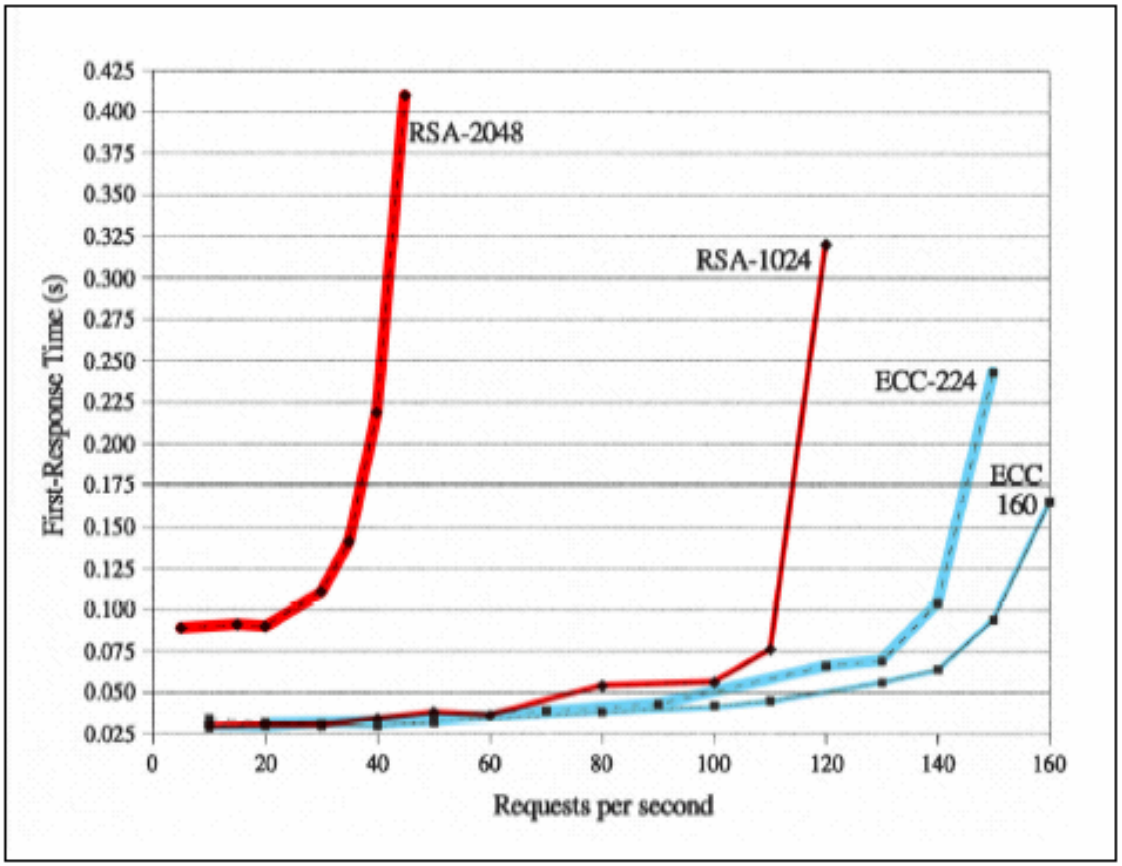
- Based on Badia's survey of Etrade, Amazon, Fidelity, Datek, Merrill Lynch and Wells Fargo
- Real world reuse
  - E.g. Shopping Cart with 66% connection reuse
  - E.g. Financial transactions with 87.5% reuse
- Real world mean page size 30 KB
- 900MHz UltraSparc III running Apache 2.0.45

Processing time reduced by 29% to 85%

Chart source: Sun Microsystems presentation to Network and Distributed System Security Symposium, 2004, Gupta, Stebila, Chang, et al. found at http://research.sun.com/projects/crypto/NDSS2004-presentation.pdf

certicom

Response Time versus Throughput



Source: Sun Microsystems

- With ECC, 30% to 270% more requests satisfied
- With ECC, roughly half the latency of RSA with high security (even under low load)

- Connection reuse 66%
- Page size 30 KB

Source: Sun Microsystems presentation to the 11th Annual Network and Distributed System Security (NDSS) Symposium, San Diego, Feb. 2004, Gupta, Stebila, Chang, et al. found at http://research.sun.com/projects/crypto/NDSS2004-presentation.pdf

certicom

certicom
securing innovation