

Integrating Elliptic Curve Cryptography (ECC) into the Web's Security Infrastructure

Vipul Gupta
Sun Microsystems, Inc
vipul.gupta@sun.com

Douglas Stebila
University of Oxford
douglas@stebila.ca

Sheueling Chang
Sun Microsystems, Inc
sheueling.chang@sun.com

<http://research.sun.com/projects/crypto>

1. Introduction

RSA is the most popular public-key cryptosystem on the Web today but long-term trends such as the proliferation of smaller, simpler devices and increasing security needs will make continued reliance on RSA more challenging over time.

We offer Elliptic Curve Cryptography (ECC) as a suitable alternative and describe our integration of this technology into several key components of the Web's security infrastructure. We also present experimental results quantifying the benefits of using ECC.

2. Need to Overhaul Internet Security

- **More and simpler devices connecting to the Web.** e.g. sensors, home appliances, personal medical devices. Many of these lack the computational resources to provide adequate security using RSA
- **More transactions requiring security.** E-commerce volume is growing rapidly. Privacy concerns will likely drive security for new kinds of transactions, e.g. book browsing at Amazon.com. These factors will significantly increase the cost of supporting RSA-based transactions.
- **Demand for higher levels of security.** Over time, computational resources available to a potential attacker increase. This will necessitate further increases in RSA key sizes and worsen the performance bottleneck.

3. Elliptic Curve Cryptography

- Public-key cryptosystem offering the highest security strength per bit. Uses smaller keys for equivalent security.
- Results in faster computations and savings in memory, power and bandwidth (especially important in constrained environments)
- Endorsed/standardized by NIST, ANSI, IEEE, IETF.

Sym-Metric	RSA/DH/DSA	ECC	Size	MIPS Yrs to attack	Protection Lifetime
80	1,024	160	6:1	10 ¹²	Until 2010
112	2,048	224	9:1	10 ²⁴	Until 2030
128	3,072	256	12:1	10 ²⁸	Beyond 2030
192	7,680	384	20:1	10 ⁴⁷	
256	15,360	521	30:1	10 ⁶⁶	

Fig 1. Equivalent key sizes (in bits) and their security strength.

4. Our Contributions

- **Driving standards** that add ECC technology to popular Internet security protocols, e.g. SSL, SSH.
- **Contributed ECC technology to open-source** cryptographic libraries (OpenSSL, Netscape Security Services aka NSS) and applications (Apache, Mozilla)
- **Demonstrated benefits of ECC** in real-world scenarios.

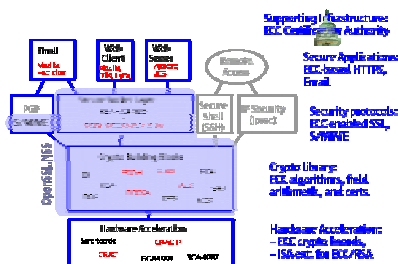


Fig 2. A systems approach to seeding ECC adoption.

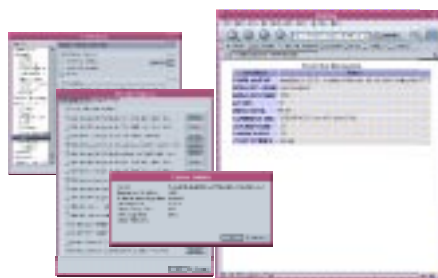


Fig 4. Mozilla communicating with an Apache web server using Elliptic Curve Cryptography.



Fig 3. Mozilla reading email signed using the Elliptic Curve Digital Signature Algorithm.

5. Performance Advantages of ECC

	ECC-160	RSA-1024	ECC-192	RSA-1536	ECC-224	RSA-2048
Time (ms)	3.69	8.75	3.87	27.47	5.12	56.18
Ops/sec	271.3	114.3	258.1	36.4	195.5	17.8
Perf ratio	2.4 : 1.0		7.1 : 1.0		11.0 : 1.0	
Key-size ratio	1.0 : 6.4		1.0 : 8.0		1.0 : 9.1	

Fig 5. ECC's performance advantage over RSA increases as security needs increase, at a rate faster than its key-size advantage.

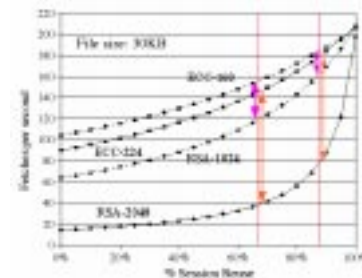


Fig 6. With ECC, a secure web server can serve 13%-31% more requests at current security levels, 120%-279% more at future levels.

Op	Avg. Time (sec)
ECC-secp160r1	1.82
ECC-secp192r1	2.82
RSA-1024 (priv)	~50
RSA-1024 (pub)	~5 (e=65537)



Fig 7. Comparison of RSA and ECC on the Berkeley "mote" sensor platform (4MHz Atmel 8-bit CPU, 128KB flash, 4KB SRAM, 4KB EEPROM).

6. Summary

- Our experiments show:
 - Significant performance benefits from using ECC in secure web transaction.
 - ECC can be used in constrained environments where traditional public-key mechanisms are simply impractical
- We have contributed this technology to OpenSSL, Apache, NSS and Mozilla with the aim of jumpstarting its widespread adoption.

Acknowledgments

The authors wish to thank Stephen Fung, Sumit Gupta, Nils Gura and Shih-Hao Hung for their help with this work.

