Advantage of using Elliptic curve cryptography in SSL/TLS

Ugur Alpay Cenar, Benjamin Clement Sebastian
ucenar@umail.ucsb.edu,benjaminclementsebastian@umail.ucsb.edu

October 31, 2015

Abstract

Mobile and wireless devices is experiencing an explosive growth. These devices have strict Power, CPU power, memory, bandwidth and latency constraints, which makes it important to have an efficient cryptosystem. It is also important for the web performance in general to have an efficient cryptosystem. Today is RSA an widely used public-key cryptosystem.The problem with RSA is that it requires large key sizes which can lead to lower bandwidth and higher CPU usage. Elliptic Curve Cryptography (ECC) is emerging as an attractive public-key cryptosystem. It offers equivalent security level with smaller key sizes, which can lead to faster computation and lower power usage.
SSL/TLS is the most widely used security protocol on the web, so more efficient SSL/TLS will have a significant impact on the web performance. This paper compares those two cryptosystems to see if ECC gives significant advantage over RSA regarding to performance when implemented in SSL/TLS protocol.

References

[1] `http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.86.6287`,

[2] `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.93.8797&rep=rep1&type=pdf`,

[3] `https://www.symantec.com/content/en/us/enterprise/white_papers/b-wp_ecc.pdf`