Using Elliptic Curve Cryptography

Yuri de Jager (s1072318)

Windesheim University of Applied Sciences

yuri.de.jager@windesheim.nl

A major change that has occurred in the cryptography field over the last decade is the development of elliptic-curve-based public-key cryptography. Although the use of elliptic curves in cryptography was suggested back in 1985, it only entered wide use in 2004 to 2005[1]. The use of elliptic curve cryptography is both faster and more secure than RSA[2] when using modern key exchange cipher suites at a comparable level of encryption.

The speed increase provided by using cipher suites based on elliptic curve cryptography is primarily based on the smaller private key size. With security in mind, a 256bit elliptic curve private key is equivalent to a 3072bit RSA private key[3]. Because modern cipher suites support Forward Secrecy (FS) [4] by using the ECDHE_RSA or ECDHE_ECDSA techniques for ephemeral key exchange[5], the importance of the size of the private key has increased. Public or session keys that are partially derived from the private key will have to be generated more frequently[6]. Benchmarks show a 60% performance increase for 256bit ECDSA key exchange compared to a 2048bit RSA key exchange[7]. A study shows that speed increases up to 200% for the key exchange and 400% when using verify operations based on elliptic curves[8].

Because of Edward Snowden's global surveillance disclosures[9] that started in 2013 and are still continuing, the use of new and proven safe encryption algorithms is, or should be, everyone's concern. Because of these disclosures it is common knowledge nowadays that intelligence agencies have actively been seeking ways to beat encryption in every possible way for many years now. This is done in order to have the encrypted data coming available to them in unencrypted form for it to be data mined. There is also a strong indication that intelligence agencies have already succeeded in beating the most commonly used encryption algorithms used on the internet[10]. The use of elliptic-curve-based cryptography is one of few possible ways left one can use to assure oneself a certain level of privacy when communicating over the Internet.

This assurance is primarily based on the fact that the use of elliptic curves in cryptography is not suggested by an intelligence agency, nor is its development influenced by an intelligence agency, but rather by two independent scientists[1]. The most commonly used cipher suites used on the Internet nowadays are based on Suite B of the NSA's promulgated cryptographic algorithms[11]. There are ongoing rumours about the NSA having lobbied for backdoors in encryptions algorithms[12] and even proposed changes to RFC's[13,14] to lower the overall security some encryption algorithms provide. Because of these facts, one could argue strongly that

independently suggested improvements[15,16] of those cryptographic algorithms, like elliptic curves, is a good thing with relation to privacy. The simple fact that elliptic curve cryptography is a relatively new cryptographic technique means that there has also been relatively little time to find weaknesses in the protocols or implementations. This provides another level of security.

Elliptic curve based cryptography should have replaced the older RSA based techniques long ago. Unfortunately, the development was slow until the beginning of the new millennium. Because of the Snowden disclosures, the cryptography field has received a lot of attention and the development of new techniques has been boosted enormously. It is time to embrace these new techniques and say goodbye to intelligence agency influenced encryption standards that date back as far as 1975. Additionally, it's worth pointing out that the NSA has already publicly made the decision to use elliptic curve cryptography back in 2009[17].

References

1) Wikipedia, *Elliptic curve cryptography*, https://en.wikipedia.org/wiki/Elliptic_curve_cryptography
2) Wikipedia, *RSA (cryptosystem)*, https://en.wikipedia.org/wiki/RSA_(cryptosystem)
3) Wikipedia, *Elliptic curve cryptography,* https://en.wikipedia.org/wiki/Elliptic_curve_cryptography#Key_sizes
4) Wikipedia, *Forward Secrecy*, https://en.wikipedia.org/wiki/Forward_secrecy
5) Wikipedia, *Elliptic curve Diffie–Hellman*, https://en.wikipedia.org/wiki/Elliptic_curve_Diffie%E2%80%93Hellman
6) Wikipedia, *Perfect Forward Secrecy*, https://en.wikipedia.org/wiki/Forward_secrecy#Perfect_forward_secrecy
7) Hubert Kario (2014), *SECURITYPITFALLS, A blog about cryptography and security*, https://securitypitfalls.wordpress.com/2014/10/06/rsa-and-ecdsa-performance/
8) Emilia Käsper (2011), *Fast Elliptic Curve Cryptography in OpenSSL*, section 4.2 *Results*, https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/37376.pdf
9) Wikipedia, *Global surveillance disclosures (2013–present)*, https://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013%E2%80%93present)
10) Wikipedia, *Bullrun (decryption program)*, https://en.wikipedia.org/wiki/Bullrun_%28decryption_program%29
11) Wikipedia, *NSA Suite B Cryptography*, https://en.wikipedia.org/wiki/NSA_Suite_B_Cryptography
12) The New York Times (2013), *Secret Documents Reveal N.S.A. Campaign Against Encryption*, http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?_r=0
13) Bruce Schneier (2007), *Did NSA Put a Secret Backdoor in New Encryption Standard?*, https://www.schneier.com/essays/archives/2007/11/did_nsa_put_a_secret.html

14) E. Roberts, Stanford University (2008), The ethics (or not) of massive government surveillance, *Encryption backdoors*, http://cs.stanford.edu/people/eroberts/cs201/projects/ethics-of-surveillance/tech_encryptionbackdoors.html
15) Wikipedia, *Neal Koblitz*, https://en.wikipedia.org/wiki/Neal_Koblitz
16) Wikipedia, *Victor S. Miller*, https://en.wikipedia.org/wiki/Victor_S._Miller
17) National Security Agency (2009), *The Case for Elliptic Curve Cryptography*, https://www.nsa.gov/business/programs/elliptic_curve.shtml