Elliptic Curve Cryptography

Suyash Patel 2015A7PS0032P

f2015032@pilani.bits-pilani.ac.in

1. Abstract

The aim of this paper is to give a basic introduction to Elliptic Curve Cryptography. I will begin by describing, very briefly, cryptographic goals and then proceed to discuss how elliptic curves have cryptographic usefulness. I would not refrain from using intricate mathematics if and when the need arises. Also an intuition would be provided as to why ECC works. Essentially the curves for which the discrete log problem is hard would be discussed. I will then introduce the problem of sending an encrypted message and discuss two encryption methods : Diffie­Hellman Key Exchange, and the Massey­Omura Encryption. I would summarise by pointing out the strengths of ECC by comparing it with RSA and other asymmetric encryption scheme and thereby, try to convince the reader that ECC is not a bad choice despite it being based on rigorous mathematical constructs. Despite the positives, ECC can be challenged by quantum computing, attacks similar to Diffie­Hellman attacks, theories of built-in backdoors and restrictions related to patents. This paper would be a serious effort to treat Elliptic Curve Cryptography in its entirety.

2. Synopsis

Before we understand the importance of Elliptic Curve Cryptography in the world of asymmetric cryptographic systems, one must understand why in the first place did one move from ciphers, like DES and AES that were doing fairly well. One of the big problems in symmetric cryptographic systems is the distribution of the secret key. The age-old problem of key distribution for symmetric ciphers does not have too many solutions and people are forced to agree to the key beforehand. Also, even if the key is agreed to beforehand, its management is cumbersome. Consider a network of N computers where every computer is connected to every other computer. One can model this by a complete graph with N nodes. This graph would have (N2-1)/2 edges and thus, as many keys. Contrast that to management of N keys in an asymmetric setting. Public key cryptography is essentially based on the idea of certain mathematical functions say, f(x) for which calculating f(x), given x, is easy but the problem of finding x given f(x) is "hard" although theoretically possible. These functions are essentially "one-way" functions.

Numerous schemes have been suggested based on known "hard"(read computationally hard) problems such as RSA, the Diffie-Hellman Exchange, its close neighbour ElGamal and so on. RSA exploits the "hard" problem of integer factorization to its constituent primes. Multiplying primes is easy but there exists no efficient algorithm for factorization. The problem of cryptanalysis of RSA translates to requiring the attacker to solve the "hard" integer factorisation problem.

Both Diffie-Hellman and ElGamal use the difficulty of solving the discrete logarithm problem effectively to create a simple key exchange scheme and a way to encrypt messages securely. ECC also relies on the "hard" discrete logarithm problem but under a different group. I would describe the discrete log problem here but its variant for the ECC would be described in the paper. To communicate securely, Alice and Bob decide on a group Zp of the prime order and an element g(non-identity) to use as the generator. Alice sends the number A = ga to Bob where a is the integer private key that she chose. Similarly, Bob sends Alice B = gb where b is Bob's chosen private key. Alice and Bob compute Ba and Ab (which are the same)respectively as the key they would use to encrypt and decrypt messages. Since, the discrete log problem is considered hard (determining a from p, g and A) an eavesdropper would feel helpless. More, formally put the discrete log problem is as follows :

Find integer *a* given only the integers *c*, *e* and *M* where *a* satisfies

ae mod M = c.

Having understood the idea that ECC tries to exploit, knowing what elliptic curves are would take us a step closer to understanding ECC. An elliptic curve over the field of real numbers is the set of points that satisfy :

y2 = x3 + ax + b.

As mentioned earlier, how discrete log problem is applied to ECC would be discussed in a separate section in the paper although the idea is to use elliptic curve groups instead of multiplicative group of integers modulo a prime.

Having loosely understood the ideas behind ECC one must realize why it is being considered in the first place. While being based on rigorous mathematical constructs ECC provides the same security as RSA does in smaller key size. ECC is most definitely strong but one must also be aware of the possible vulnerabilities and be careful while making choices. One such choice that the one who implements ECC makes is choosing an elliptic curve. There exists a general method of attack that runs in sqrt(n) time but that is slow. There are few specific classes of elliptic curves for which discrete log problem becomes easy like supersingular curves but it is easy to pick curves that do not fall in such classes. ECC is an theoretically interesting field.