Scribe: Cryptography and Network Security (Week11.Class2.A)

Juluri Shree Shiva Teja

12-Nov-2020

1 Introduction

The following scribe describes about the techniques of Elliptic Curve Cryptography and its practical usage.

2 Elliptic Curve Cryptography (ECC)

It is a public key cryptosystem in which public key is used for encryption and private key is used for decryption. The mathematical operation underlying ECC is point multiplication which is nothing but repeated addition of two points.

2.1 Generic Procedures

In the elliptic curve equation,

$$y^2 = x^3 + ax + b$$

the values of a, b are publicly choosen. The prime field p is also public. A base point B is choosen to generate all other points from the elliptic group which is also public. A private key x is choosen and a public key Q is defined as product of x and B both for sender and receiver separately.
Example: Consider El Gamal system where Alice wants to send an encrypted message to Bob. Then Alice has a private key a and public key $P_a = a * B$, Bob has a private key b and public key $P_b = b*B$ where B is the mutually agreed base point. The message M Alice wants to send is mapped into a point P_M on elliptic curve. The El Gamal system is analogous to Elliptic curve where exponentiation α^r is replaced by scalar multiplication r*P (point addition). During encryption, the ciphertext is computed with a random number k and sent to Bob as

$$P_c = [(kB), (P_M + kP_B)]$$

Hence the information of P_M is hided by random number k. During decryption, as Bob knows private key b, hence the following computation can be performed

from the ciphertext

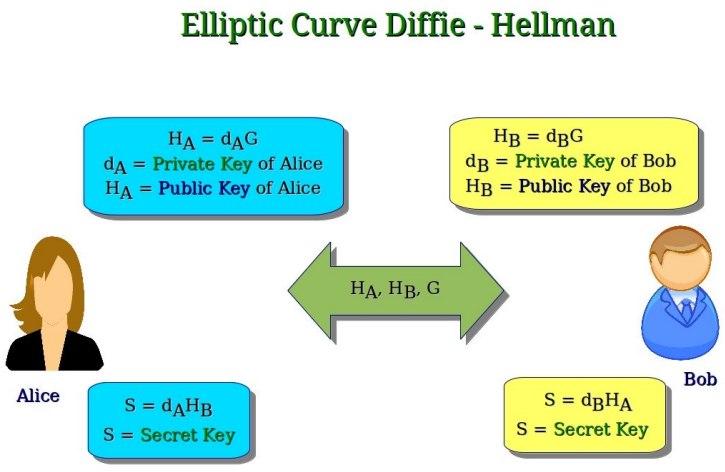
$$(P_M + kP_B) - [b * (kB)] = P_M + [k * (bB)] - [k * (bB)] = P_M$$

Note: b*(kB)=k*(bB) because both k and b are scalars. Hence, P_M can be obtained by decryption.

3 Encoding of a message on Elliptic curve

The plaintext is assumed to contain numbers and English characters. Numbers are encoded the same 0-9 and 26 English characters are encoded 10-35. For encryption of the message m, a public variable k is choosen such that x=mk+i for i in range of [1,k-1] for which y is an integral value. Such value of (x,y) is the point on the curve to which m is encoded. For the decryption, we have message m=(x-i)/k, but the value of i is unknown. But the range of i is known to be [0,k-1] which indicates that m=floor value of (x-1)/k. Hence decryption is very simple.
Note: For every value of i, the computed y may not be integral value. Among all the p possible residues, probability that the obtained residue is a quadratic residue is 1/2. So, the probability of failure to find an integral y is $\frac{1}{2^{k-1}}$. Hence, the higher the value of k, the better we can find the value of i such that y is an integral value. k=20 is good enough for our purpose.

4 Diffie-Hellman (DH) Key Exchange



5 Uses of ECC

The mathematical computation involved in a particular encryption and the algorithm followed for encryption and decryption determines how secure is the cryptosystem. For example, integer factorization in RSA, discrete logarithms in DH, elliptic curve discrete logarithm problem in ECC. ECC algorithm results in shorter key sizes which is efficient approach leading to same level of security. Hence, it has wide range of applications in systems constrained to storage, computation power etc.

6 Elliptic curve discrete log problem (ECDLP)

ECDLP is harder than DLP problem but its time complexity is more.
Algorithm: Consider 2 lists of size r generated by choosing random integers between 1 and p.
List L1: j_1P, j_2P.....j_rP
List L2: k_1P+Q, k_2P+Q.....k_rP+Q
For any collision between the lists, we have
$\Rightarrow j_uP = k_vP + Q \Rightarrow Q = (j_u - k_v)P$
So, with a probability of r=O($p^{1/2}$), there is a probability of collision. Hence the time complexity is also the same. So the choice of algorithm depends on time and space complexity tradeoff.

7 Conclusion

ECC is efficient secure encryption algorithm which relies on hardness of elliptic curve logarithm problem. Elliptic curves are applicable for key agreement, digital signatures, pseudo-random generators and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a symmetric encryption scheme.