Lecture 30 - ECDSA - Elliptic curve public key encryption

Videos (part 1 .. 3)

https://youtu.be/0x1NNdEC2d4 - Lect-30-4010-pt1-ECDSA.mp4
https://youtu.be/AZDUaOlbGLM - Lect-30-4010-pt2-add-double-mul.mp4
https://youtu.be/qsoh50Ls8B4 - Lect-30-4010-pt3-discreet.mp4

From Amazon S3 - for download (same as youtube videos)

http://uw-s20-2015.s3.amazonaws.com/Lect-30-4010-pt1-ECDSA.mp4
http://uw-s20-2015.s3.amazonaws.com/Lect-30-4010-pt2-add-double-mul.mp4
http://uw-s20-2015.s3.amazonaws.com/Lect-30-4010-pt3-discreet.mp4

EC and ECDSA Encryption

How ECDSA works under the covers

Eliptic Curve Function

The general equation for elliptic curves is:

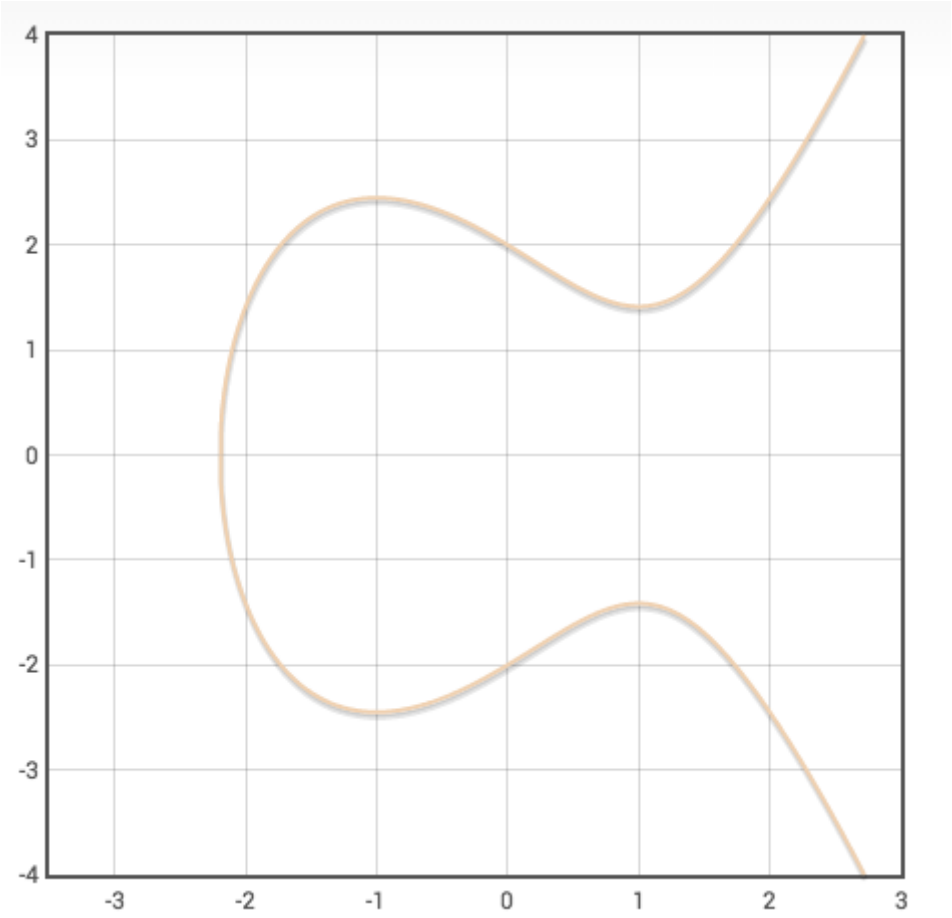
$$y^2 = x^3 + a * x + b$$

This specific elliptic curve has equation:

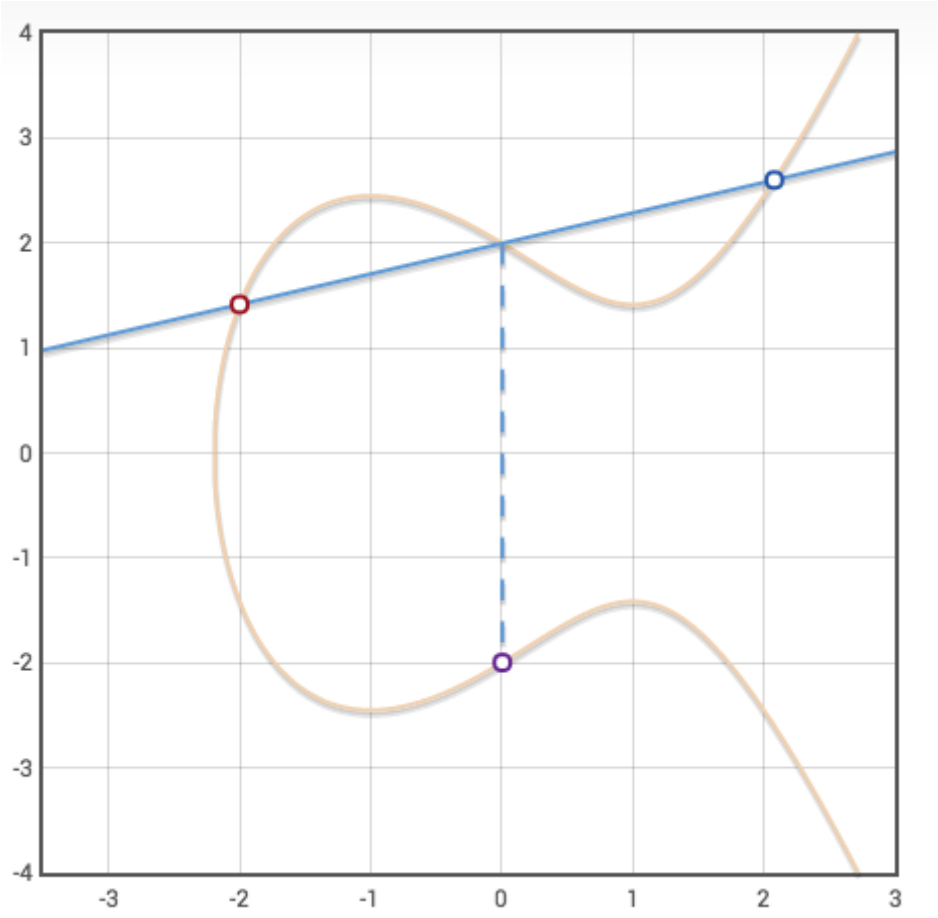
$$y^2 = x^3 - 3 * x + 4$$

All elliptic curves are symmetric about the x-axis.

Graphed



Good EC, bad EC, addition.

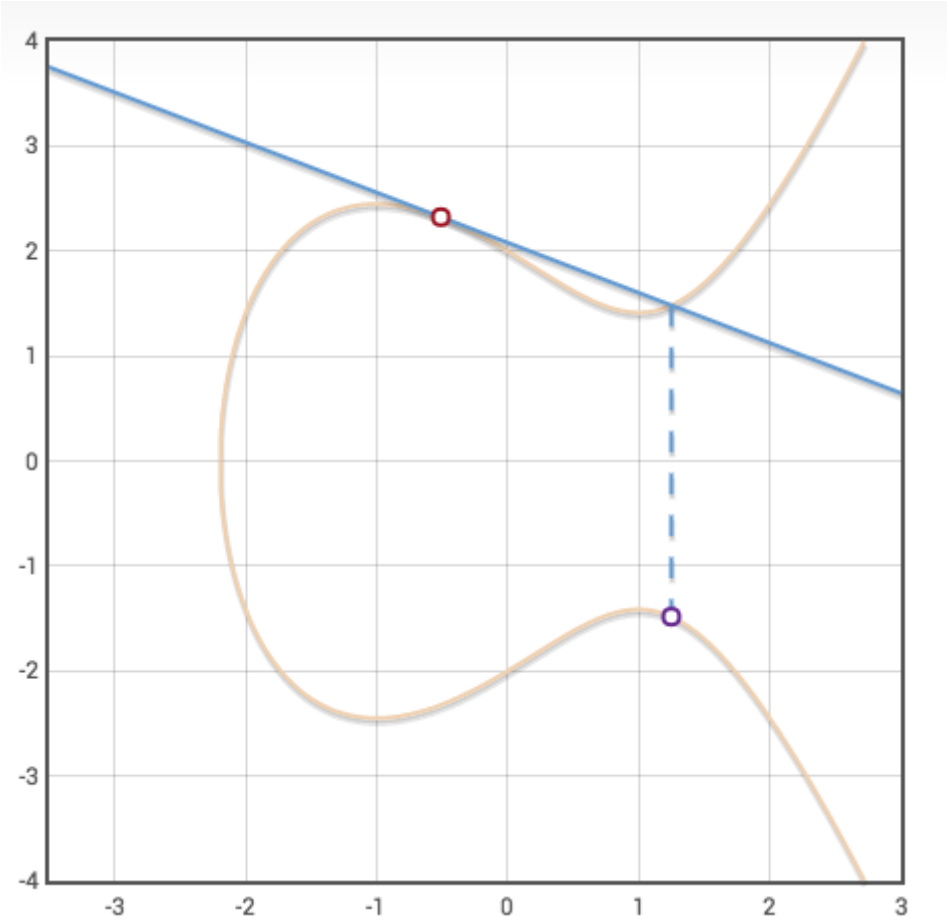


To add 2 points (Point A, and Point B)

1. Draw a line between Point A and Point B
2. This line always intersects the elliptic curve at a 3rd point.
3. Reflect the the observed intersection point over the x axis to get the sum of Point A and Point B

$$(-2.0, 1.4) + (2.0, 2.5) = (0.0, -1.9)$$

Doubleling of a value.



To double a point (Point A + Point A)

1. Draw a line tangent to the elliptic curve through Point A
2. This line always intersects the elliptic curve at a 2nd point.
3. Reflect the the observed intersection point over the x axis to get 2 * Point A

$$2 * (-0.5, 2.3) = (1.2, -1.4)$$

Given $(x_1, y_1), (x_2, y_2)$: to find $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$

$$x_3 = s^2 - x_1 - x_2$$
$$y_3 = s(x_1 - x_3) - y_1$$

$$s = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{if } (x_1, y_1) \neq (x_2, y_2) \\ \frac{3x^2 + a}{2y_1}, & \text{if } (x_1, y_1) = (x_2, y_2) \end{cases}$$

$$\text{Point A} + \text{Point B} = \text{Point C}$$

$$2 * \text{Point A} = \text{Point 2A}$$

Because multiplication is just addition many times, we also have multiplication:

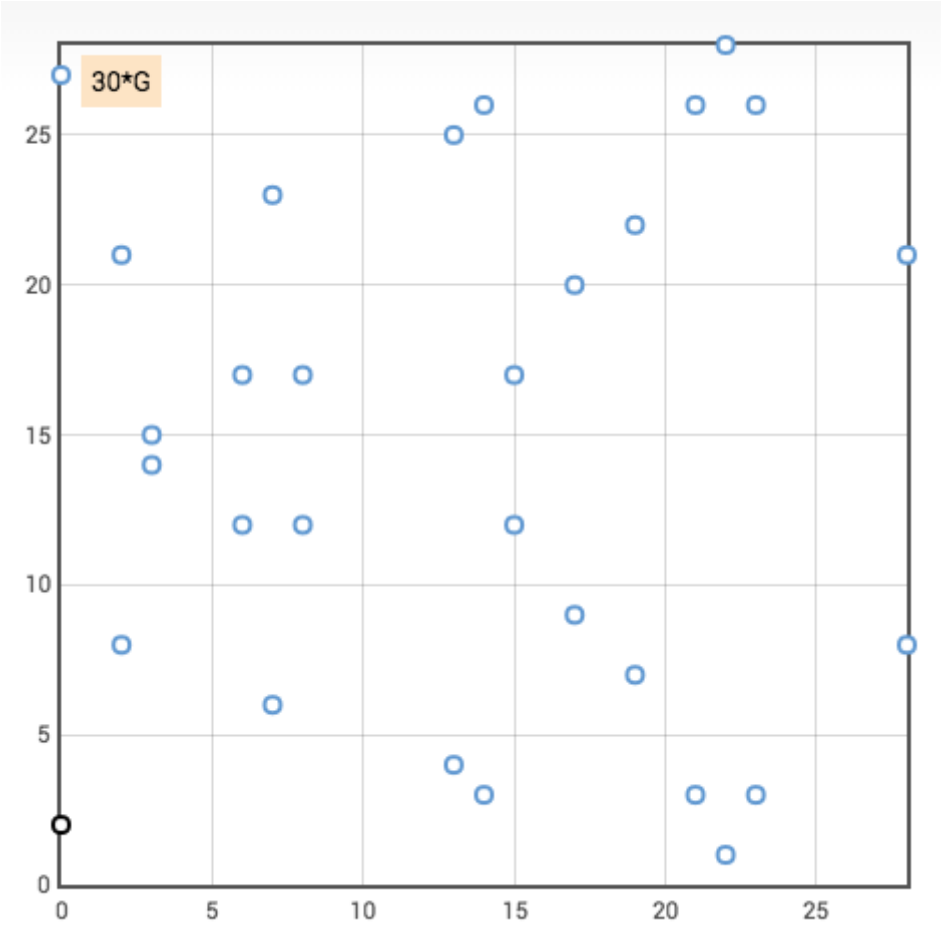
$$\text{Point A} + \text{Point A} + \cdots + \text{Point A} = N * \text{Point A}$$

$$N * \text{Point A} = \text{Point NA}$$

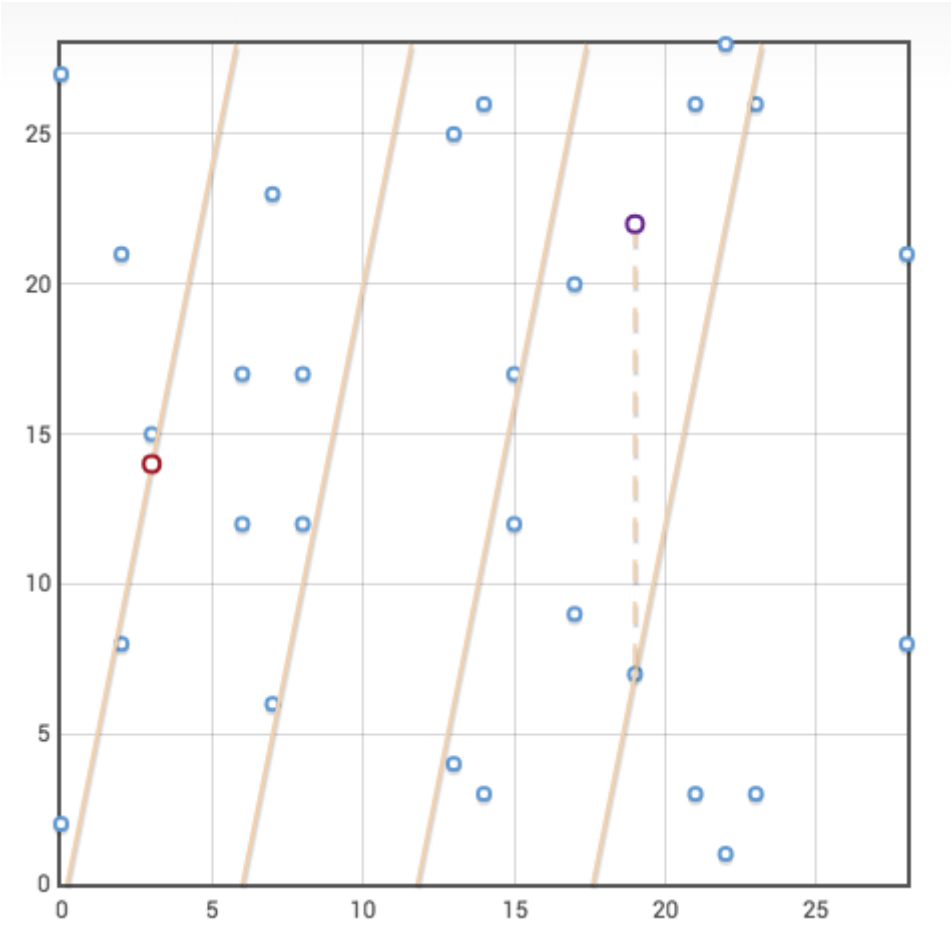
$$7 * \frac{1}{7} = 1$$

$$7 * 2 \bmod 13 = 1$$

As integers we get:



Now we can use a modulo system for this:



$$2 * (3, 14) = (19, 22)$$

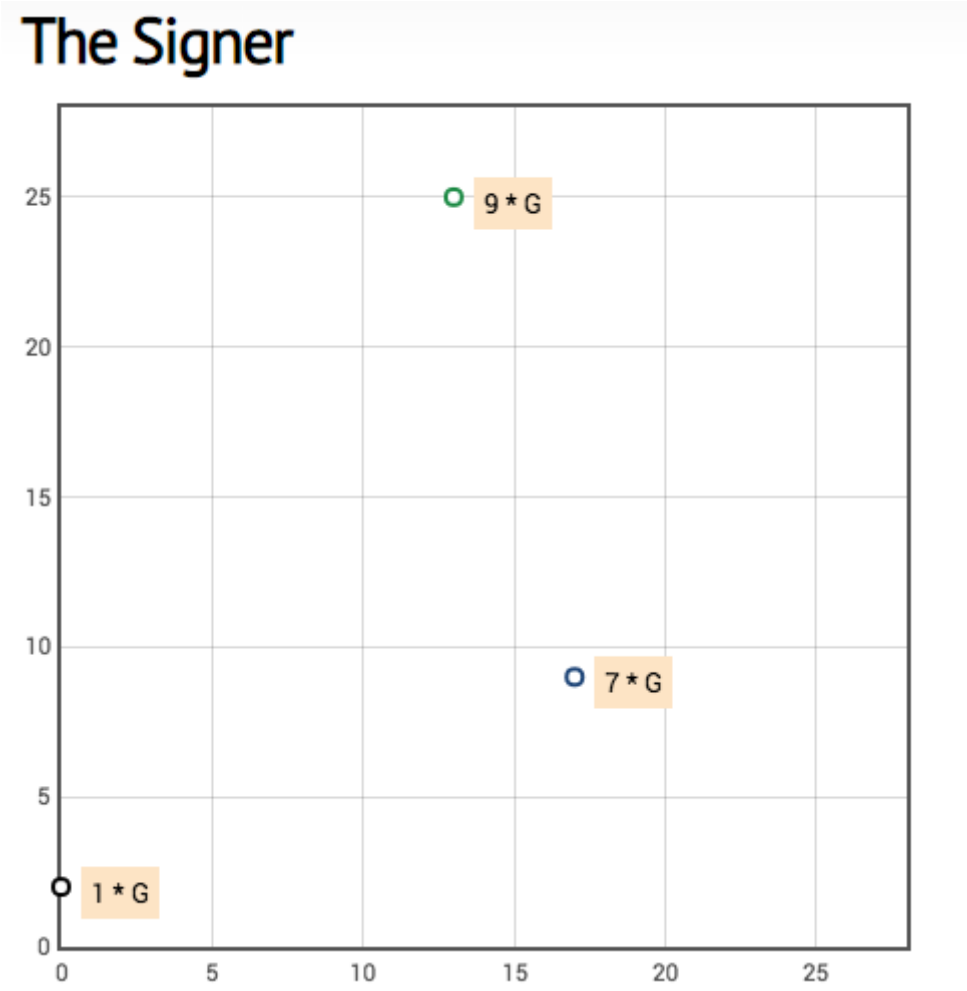
$$(3, 14) = 21 * G$$

$$(19, 22) = 11 * G$$

$$11 = 2 * 21 \bmod 31$$

$$\text{Private Key} * G = \text{(Public Key)}$$

Private key is the generator multiplier (an integer).
G is the generator point, it is publicly known and is the same for everyone.
Public key is the point generated by the private key.


The Signer
9 * G
7 * G
1 * G
0
5
10
15
20
25

The signer knows:

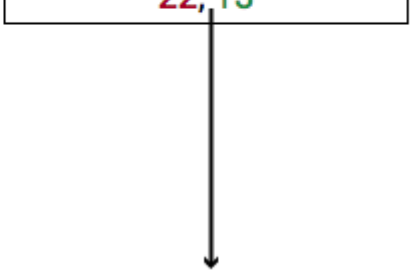
Generator:	1 * G = (0, 2)
Private Key:	7 * G = (17, 9)
Random Point:	9 * G = (13, 25)
Message Hash:	14

Signature Factor:

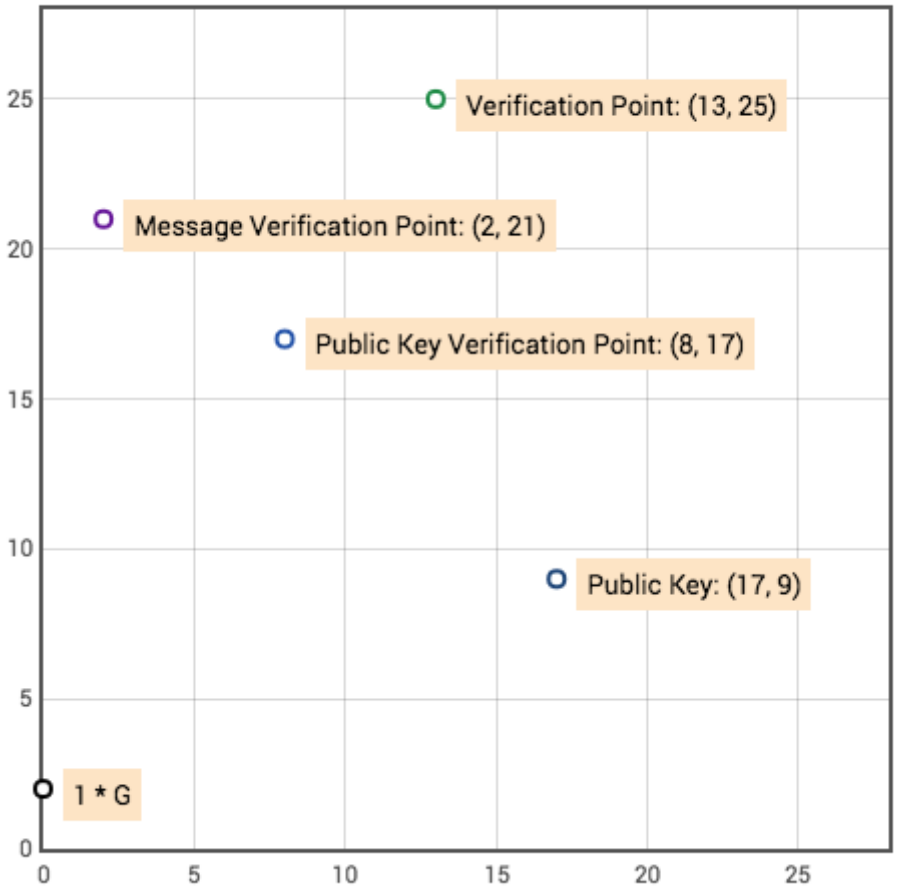
$$22 = \frac{14 + 13 * 7}{9} \bmod 31$$

The Signature

22, 13



The Verifier



The verifier knows:

Generator: 1 * G = (0, 2)

Public Key: (17, 9)

Signature Factor: 22

Message Hash: 14

Message Verification Point:

$$(2, 21) = \frac{14}{22} \bmod 31 \ * (0, 2)$$

Public Key Verification Point:

$$(8, 17) = \frac{13}{22} \bmod 31 \ * (17, 9)$$

Verification Point:

$$(2, 21) + (8, 17) = (13, 25)$$