Homework 4: Unerstanding ECC
ECC and ECDH explained

CNS Course Sapienza

Riccardo Salvalaggio 1750157

15/11/2020

1 Introduction

In the last report (on RSA) I talked about the division of the cryptography world into: Symmetric and Asymmetric ciphers. Anyway, they are also known as Private and Public key.
Today, I am going to explain a particular approach to Asymmetric ones: Elliptic-curve cryptography (ECC) and its application with DH based on Prof. Christof Paar brilliant lectures (As a tribute I will divide ins sections as He did in lectures).
ECC is an approach based on the algebraic structure of elliptic curves over finite fields.
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.

2 Introduction to Elliptic Curves (EC)

Talking about cryptography, we have 2 principal Cryptosystem applicable to EC: ECDH (we'll talk about it later), ECDSA, both with security levels: 160, 256, 384, 512 bits.

Algorithm Family	Cryptosystems	Security Level (bit)			
		80	128	192	256
Integer factorization	RSA	1024 bit	3072 bit	7680 bit	15360 bit
Discrete logarithm	DH, DSA, Elgamal	1024 bit	3072 bit	7680 bit	15360 bit
Elliptic curves	ECDH, ECDSA	160 bit	256 bit	384 bit	512 bit
Symmetric-key	AES, 3DES	80 bit	128 bit	192 bit	256 bit

Not to be confused with Ellipse.
Background Idea: Can we find another cyclic group in which the DLP is almost computationally impossible?
Let's look at Polynomials: $x^2 + y^2 = z^2 \rightarrow$ circumference
start adding coefficient: $ax^2 + by^2 = z^2 \rightarrow$ ellipse
For the use we need in crypto we consider polynomials over Zp (the set of integer number from 0 to p-1).
After this preamble we get that: elliptic curves over Zp, p>3, is the set of pairs (x,y) in Zp:

$$y^2 = x^3 + ax + b \text{ mod p}$$

together with an imaginary point at infinity.

If we use purely mathematical (theoretical) models is really hard to understand and it looks very abstract. Instead, Elliptic curve has a really nice geometric interpretation. With modulo operation the graphical interpretation completely collapses, so we are going over R.
Note: if we look w.r.t. the X axis, we see symmetry.

For next sections we follow this definition of group:
"A group is a set of elements G together with an operation ∘ which combines two elements of G. A group has the following properties:
1. The group operation ∘ is closed. That is, for all a,b,in G, it holds that a∘b=c in G.
2. The group operation is associative. That is, a∘(b∘c)=(a∘b)∘c for all a,b,c in G.
3. There is an element 1 in G, called the neutral element(or identity element), such that a∘1=1∘a=a for all a in G.
4. For each a in G there exists an element a-1 in G, called the inverse of a,

such that a∘a-1=a-1∘a=1.

5. A group G is abelian (or commutative)if, furthermore, a∘b=b∘a for all a,b in G."

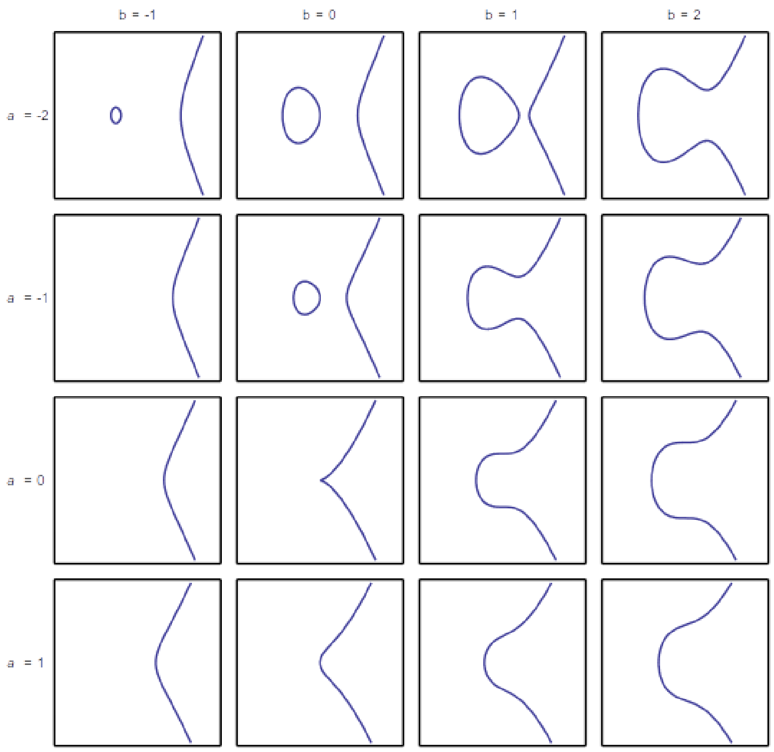

Figure 1: Different shapes of Elliptic curves based on different values of a and b.

3 Group operations [in Zp* a b mod p]

Q: Analytical expression for the group operation ? EC point addition and doubling.

Elliptic Curve Point Addition and Point Doubling

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

where

$$s = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \bmod p \text{ ; if } P \neq Q \text{ (point addition)} \\ \frac{3x_1^2 + a}{2y_1} \bmod p \text{ ; if } P = Q \text{ (point doubling)} \end{cases}$$

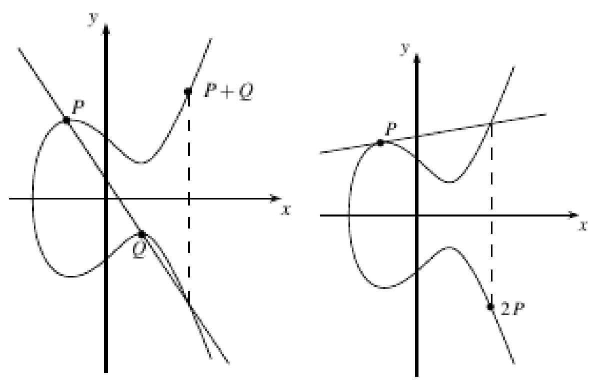

Figure 2: Point addition and point doubling.

Point addition: P+Q = R (P!=Q). Draw a line through P and Q and obtain a third point of intersection between the elliptic curve and the line. Mirror this third intersection point along the x-axis.
Point doubling: P+P = 2P. We draw the tangent line through P and obtain a second point of intersection between this line and the elliptic curve. We mirror the point of the second intersection along the x-axis.
Ex.
We have E: $y^2 = x^3 + 2x + 2$ mod 17
We want to double P = (5,1)
2P = P + P = (5,1)+(5,1) = (x3,y3)
s = $(3x1^2 + alfa)/2y1 = (2 * 1) - 1(3 * 52 + 2) = 2 - 1 * 9 = 9 * 9 = 13$ mod 17
x3 = $s^2 - x1 - x2$ = 169–5–5 = 159 = 6 mod 17

y3 = s(x1 − x3) − y1 = 13(5-6)-1 = -14 =3 mod 17
2P = (5,1)+(5,1) = (6,3)

We check that 2P is a point on the curve:
$y^2 = x^3 + 2x + 2$ mod 17
$3^2 = 6^3 + 2 * 6 + 2$ mod 17
9 = 230 = 9 mod 17

Q: What is the neutral element?
It's an element such that: P + ? = P for all P
we Define a "point at infinity", following the definitions of group:
Property 3: P + 0 = P for all P in E
Property 4: P + (-P) = 0 for all P in E
We can also define the contrary of P=(x,y) that is by definition -P = (x,-y)
Note: the points on an EC, including infinity, have cyclic subgroups.

Finally, the cyclic subgroup is defined by its generator G. For cryptographic application the order of G, that is the smallest positive number n such that n*G = point at infinity, is normally prime.

4 EC DLP

Ex. EC as a cyclic group
E: $y^2 = x^3 + 2x + 2$ mod 17, for this specific curve, all points form a cyclic group.
Primitive element P=(5,1)
2P=P+P=...=(6,3)
3P=2P+P=...=(10,6)
. . .
18P=(5,16) ← =(5,-1)=-P (mod 17)
19P=18P+P=(5,16)+(5,1)
= -P+P= Neutral element (infinity)
20P=19P+P= infinity + P= P
21P=20P+P=P+P=2P
22P=21P+P=2P+P=3P
. . .

We obtain immediately a **discrete logarithm problem**

Elliptic Curved Discrete Logarithm Problem (ECDLP).
Given is an elliptic curve E. We consider a primitive element P and another element T. The DL problem is finding the integer d, where 1 <= d <= |E|, such that: P+P+···+P (d times) =d*P=T.
It is also called point multiplication, since we can formally write T=d*P.
As we introduced before, in cryptosystems, d is the private key which is an integer, while the public key T is a point on the curve with coordinates T=(x^T, y^T).
In contrast, in the case of the DL problem in Z*p, both keys were integers.
Note about EC DLP:

d=K_{pr} integer (always)

T=K_{pub} point on curve, i.e. a group element.

Q: Group cardinality of E?
=> |E| = 19 (We can see that 20P is again P).

Hasse's theorem.
Given an elliptic curve E modulo p, the number of points on the curve is denoted by |E| and is bounded by:

$$p+1-2*\sqrt{p} <= |E| <= p+1+2*\sqrt{p}.$$

Hasse's theorem gives us a lower + upper bound for E. For extremely huge value of p we can do a very rough approximation: |E| p.
It can seem wrong (and under a certain point of view it is, in fact in practice we don't use this approximation), but the sense is that, since |E| is bounded by p + or − small quantities related to p, for enormous value of p this small quantities are irrelevant.

Q: How hard is ECDLP?
If the EC is chosen carefully, the best known algorithm for computing the EC DLP requires $\sqrt{p}$ steps (there are not few).
Ex. p x 2160
Attack requires: $\sqrt{p}$ $\sqrt{2160}$=2160/2=280 steps

5 EC Diffie-Hellman Key Exchange (ECDH)

Straightforward adoption of DH in Zp.
Key exchange is composed of two phases:
I) Set-up

$$\text{Elliptic curve E: } y^2 = x^3 + ax + b \text{ mod p}$$

$$\text{primitive element P (xp,yp)}$$

II) Protocol

Elliptic Curve Diffie–Hellman Key Exchange (ECDH)

Alice		Bob
choose $k_{prA} = a \in \{2, 3, \ldots, \#E - 1\}$		choose $k_{prB} = b \in \{2, 3, \ldots, \#E - 1\}$
compute $k_{pubA} = aP = A = (x_A, y_A)$		compute $k_{pubB} = bP = B = (x_B, y_B)$
	$\xrightarrow{A}$	
	$\xleftarrow{B}$	
compute $aB = T_{AB}$		compute $bA = T_{AB}$

Joint secret between Alice and Bob: $T_{AB} = (x_{AB}, y_{AB})$.

Ex.

Alice		Bob
choose $a = k_{pr,A} = 3$		choose $b = k_{pr,B} = 10$
$A = k_{pub,A} = 3P = (10, 6)$		$B = k_{pub,B} = 10P = (7, 11)$
	$\xrightarrow{A}$	
	$\xleftarrow{B}$	
$T_{AB} = aB = 3(7, 11) = (13, 10)$		$T_{AB} = bA = 10(10, 6) = (13, 10)$

Q:How to compute a*P = P + P + P.... (a times)
In elliptic curve square becomes doubling $\rightarrow$ P2= P+P
The "point multiplication" a*P can be computed with the "double-and-add" algorithm.
Ex. 26P = ?
26P = (11010_2)P 1 step for every bit that compose 11010
Step

0) P = 1_2 P
1a) P+P = 2P = 10_2 P Doubled (because the second bit of P is not 0)
1b) 2P+P = 3P = 11_2P Add (now the combination is right).
2a) 3P+3P=6P=110_2P Doubled
3a) 6P+6P=12P=1100_2P Doubled
3b) 12P+P=13P=1101_2P now we have the real combination so Add

4a) 13P+13P=26P=11010_2P Doubled

It can be summarized by this algorithm:

Double-and-Add Algorithm for Point Multiplication
Input: elliptic curve E together with an elliptic curve point P
a scalar $d = \sum_{i=0}^{t} d_i 2^i$ with $d_i \in 0, 1$ and $d_t = 1$
Output: $T = dP$
Initialization:
$T = P$
Algorithm:
1 FOR $i = t - 1$ DOWNTO 0
1.1 $T = T + T \bmod n$
IF $d_i = 1$
1.2 $T = T + P \bmod n$
2 RETURN (T)

References

[1] Lecture 16: Introduction to Elliptic Curves by Christof Paar

[2] Lecture 17: Elliptic Curve Cryptography (ECC) by Christof Paar [Video]

[3] Wikipedia: ECC ECDH