PKIs and Elliptic Curves

Douglas Wikström
KTH Stockholm
`dog@csc.kth.se`

February 28

- PKIs

- Elliptic Curves

Problem

- We have constructed public-key cryptosystems and signature schemes.

- Only the holder of the secret key can decrypt ciphertexts and sign messages.

- How do we **know** who holds the secret key corresponding to a public key?

Signing Public Keys of Others

▶ Suppose that Alice computes a signature
$\sigma_{A,B} = \mathsf{Sign}_{\mathsf{sk}_A}(\mathsf{pk}_B, Bob)$ of Bob's public key pk_B and his identity and hands it to Bob.

▶ Suppose that Eve holds Alice's public key pk_A.

▶ Then **anybody** can hand $(\mathsf{pk}_B, \sigma_{A,B})$ **directly** to Eve, and Eve will be convinced that pk_B is Bob's key (assuming she trusts Alice).

Certificate

- A **certificate** is a signature of a public key along with some information on how the key may be used, e.g., it may allow the holder to issue certificates.

- A certificate is valid for a given setting if the signature is valid and the usage information in the certificate matches that of the setting.

- Some parties must be trusted to issue certificates. These parties are called Certificate Authorities (CA).

Certificate Chains

A CA may be "distributed" using in certificate chains.

- Suppose that Bob holds valid certificates

$$\sigma_{0,1}, \sigma_{1,2}, \ldots, \sigma_{n-1,n}$$

where $\sigma_{i-1,i}$ is a certificate of pk_{P_i} by P_{i-1}.

- Bob must trust all parties in the chain[1].

---

[1]Sometimes he can point out a cheater if at least the root is honest.

Groups

- ▶ We have argued that discrete logarithm problems are hard in large subgroups of $\mathbb{Z}_p^*$ and $\mathbb{F}_q^*$.

- ▶ Based on discrete logarithm problems (DL, DH, DDH) we have shown how to construct public key cryptosystems, key exchange protocols, and signature schemes.

- ▶ An elliptic curve is yet another candidate of a group where discrete logarithm problems are hard.

Motivation For Studying Elliptic Curves

- ▶ What if it turns out that solving discrete logarithms in $\mathbb{Z}_p^*$ is easy? Elliptic curves give an **alternative**.

- ▶ The best known DL-algorithms in an elliptic curve group with prime order q are **generic algorithms**, i.e., they have running time $O(\sqrt{q})$

- ▶ Arguably we can use **shorter keys**. This is very important in some practical applications.

Definition

Definition. A plane cubic curve E (on Weierstrass form) over a field $\mathbb{F}$ is given by a polynomial

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

with $a, b \in \mathbb{F}$. The set of points (x, y) that satisfy this equation over $\mathbb{F}$ is written $E(\mathbb{F})$.

Definition

Definition. A plane cubic curve E (on Weierstrass form) over a field $\mathbb{F}$ is given by a polynomial

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

with $a, b \in \mathbb{F}$. The set of points (x, y) that satisfy this equation over $\mathbb{F}$ is written $E(\mathbb{F})$.

Every plane cubic curve over a field of characteristic $\neq 2, 3$ can be written on the above form without changing any properties we care about.

Alternative Notation

We also write

$$g(x, y) = y^2 - x^3 + ax + b \quad \text{or}$$
$$y^2 = f(x)$$

where $f(x) = x^3 + ax + b$.

Singular Points

Definition. A point $(u, v) \in E(\mathbb{E})$, with $\mathbb{E}$ an extension field of $\mathbb{F}$, is **singular** if

$$\frac{\partial g(x, y)}{\partial x}(u, v) = \frac{\partial g(x, y)}{\partial y}(u, v) = 0 \ .$$

Definition. A plane cubic curve is **smooth** if $E(\overline{\mathbb{F}})$ contains no singular points[2].

---

[2] $\overline{\mathbb{F}}$ is the algebraic closure of $\mathbb{F}$.

What Does This Mean?

Note that

$$\frac{\partial g(x,y)}{\partial x}(x,y) = f'(x) = 3x^2 + a \quad \text{and}$$
$$\frac{\partial g(x,y)}{\partial y}(x,y) = 2y \ .$$

Thus, any singular point $(u,v) \in E(\mathbb{F})$ must have:

- $v = 0$,
- $f(u) = 0$, and $f'(u) = 0$.

Then $f(x) = (x-u)h(x)$ and $f'(x) = h(x) + (x-u)h'(x)$, so (u,v) is singular if $v = 0$ and u is a double-root of f.

Discriminant

In general a "discriminant" can be used to check if a polynomial has a double root.

Definition. The discriminant $\Delta(E)$ of a plane curve $y^2 = x^3 + ax + b$ is given by $-4a^3 - 27b^2$.

Lemma. The polynomial $f(x)$ does not have a double root iff $\Delta(E) \neq 0$, in which case the curve is called **smooth**.

Line Defined By Two Points On Curve

Let $l(x)$ be a line that intersects the curve in (u_1, v_1) and (u_2, v_2).
Then
$$l(x) = k(x - u_1) + v_1$$

where
$$k = \begin{cases} \frac{v_2 - v_1}{u_2 - u_1} & \text{if } (u_1, v_1) \neq (u_2, v_2) \\ \frac{3u_1^2 + a}{2v_1} & \text{otherwise} \end{cases}$$

Line Defined By Two Points On Curve

Let $l(x)$ be a line that intersects the curve in (u_1, v_1) and (u_2, v_2).
Then

$$l(x) = k(x - u_1) + v_1$$

where

$$k = \begin{cases} \frac{v_2 - v_1}{u_2 - u_1} & \text{if } (u_1, v_1) \neq (u_2, v_2) \\ \frac{3u_1^2 + a}{2v_1} & \text{otherwise} \end{cases}$$

We are cheating a little here in that we assume that $u_1 \neq u_2$ and
$v_1 \neq 0$. In both such cases we get a line parallel with $x = 0$ that
we deal with in a special way.

Finding the Third Point

▶ The intersection points between $l(x)$ and the curve are given
   by the zeros of

$$t(x) = g(l(x), x) = l(x)^2 - f(x)$$

which is a cubic polynomial with known roots u_1 and u_2.

Finding the Third Point

- ▶ The intersection points between $l(x)$ and the curve are given by the zeros of

$$t(x) = g(l(x), x) = l(x)^2 - f(x)$$

  which is a cubic polynomial with known roots u_1 and u_2.

- ▶ To find the third intersection point (u_3, v_3) we note that

$$t(x) = (x - u_1)(x - u_2)(x - u_3) = x^3 - (u_1 + u_2 + u_3)x^2 + r(x)$$

  where $r(x)$ is linear. Thus, we can find u_3 from t's coefficients!

From Intersection Points To Group Law

- ▶ Given any two points A and B the on the curve that defines a line, we can find a third intersection point C with the curve (even if $A = B$).

From Intersection Points To Group Law

- ▶ Given any two points A and B the on the curve that defines a line, we can find a third intersection point C with the curve (even if $A = B$).

- ▶ The only exception is if our line $l(x)$ is parallel with the y-axis.

From Intersection Points To Group Law

▶ Given any two points A and B the on the curve that defines a line, we can find a third intersection point C with the curve (even if $A = B$).

▶ The only exception is if our line $l(x)$ is parallel with the y-axis.

▶ To "fix" this exception we add a point at infinity O, roughly at $(0, \infty)$ (the projective plane). Intuition: the sides of a long straight road seem intersect infinitely far away.

From Intersection Points To Group Law

- We define the sum of A and B by $(x, -y)$, where (x, y) is the third intersection point of the line defined by A and B with the curve.

- We define the inverse of (x, y) by $(x, -y)$.

- The main technical difficulty in proving that this gives a group is to prove the associative law. This can be done with Bezout's theorem, or by (tedious) elementary algebraic manipulation.

Elliptic Curves

- There are many elliptic curves with special properties.

- There are many ways to implement curves as well as the underlying field.

- More requirements than smoothness must be satisfied for a curve to be suitable for cryptographic use. There are suitable standardized curves.