Elliptic Curves and Cryptography

By K.Draziotis
Informatic's Department
Aristotle University of Thessaloniki

90 years of
Mathematics in the
Aristotle University of Thessaloniki

- Outline

- Elliptic curves – formal definition
- Elliptic curves over
- Group Law (chord-tangent method)
- Doubling a point : P+P=R
- How the group E(K) looks like?
- The free part
- Meaning of the rank
- Birch and Swinnerton-Dyer Conjecture (1960 - 1965)
- BSD, a million dollar problem
- The torsion part
- The torsion part
- An example
- Order of a point P
- The group of order m, E[m]
- The Group structure of the elliptic curve
- Example
- DLP over a Group
- Diffie-Hellman protocol
- Also Bitcoin protocol uses ECC
- ECC
- ECDLP
- An example
- Not only exchanging messages with elliptic curves
- Attacks to (EC)DLP in a group G
- Attacks in the multiplicative group modulo p
- Cases where ECDLP is easy
- Pairing based cryptography
- Pairings
- Quantum attacks to ECDLP
- Quantum resistant ECC
- SIDH
- References

- Elliptic curves have many applications in many areas of mathematics. From number theory to complex analysis and from cryptography to physics.

- **Number theory** : FLT, BSD conjecture
- **Physics** : paths of strings looks like elliptic curves
- **Cryptography** : Lenstra factorization, Primality test, Diffie-Hellman, Pairing cryptography, Post Quantum protocols (SIDH)
- **Mathematical analysis** : computation of elliptic integrals $\int_a^b R(x,y)dx, y^2 = cubic$

The inverse function(elliptic integral) of

$$f(y) = \int_y^\infty \frac{1}{\sqrt{4t^3 - g_2 t - g_3}} dt$$

is $y = \wp(z)$

Elliptic curves – formal definition

Definition

An elliptic curve E over a field **K** is defined by an equation

$$\mathrm{E} : \mathrm{y}^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in \mathbf{K}$$

and has discriminant Δ non zero.

Its discriminant is given by the formula

$$\Delta = -d_2^2d_8 - 8d_4^2 - 27d_6^2 + 9d_2d_4d_6$$

$$d_2 = a_1^2 + 4a_2 \qquad d_6 = a_3^2 + 4a_6$$

$$d_4 = 2a_4 + a_1a_3 \quad d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$

- This equation is called Weierstrass equation.
- The condition $\Delta \neq 0$ ensures that the curves does not have singular points, i.e. points where there are more than one distinct tangents
- Sometimes we write E/**K** to denote that E is defined over **K,** i.e. the coefficients are in the field **K**.
- Also, there is only one point at infinity $\infty = [0:1:0]$
- If $cha(K) \neq 2,3$ there is a change of variables that transforms E to $y^2 = x^3 + Ax + B$ and

$$A,\ B \in \mathbf{K}, \Delta = -16(4A^3 + 27B^2)$$

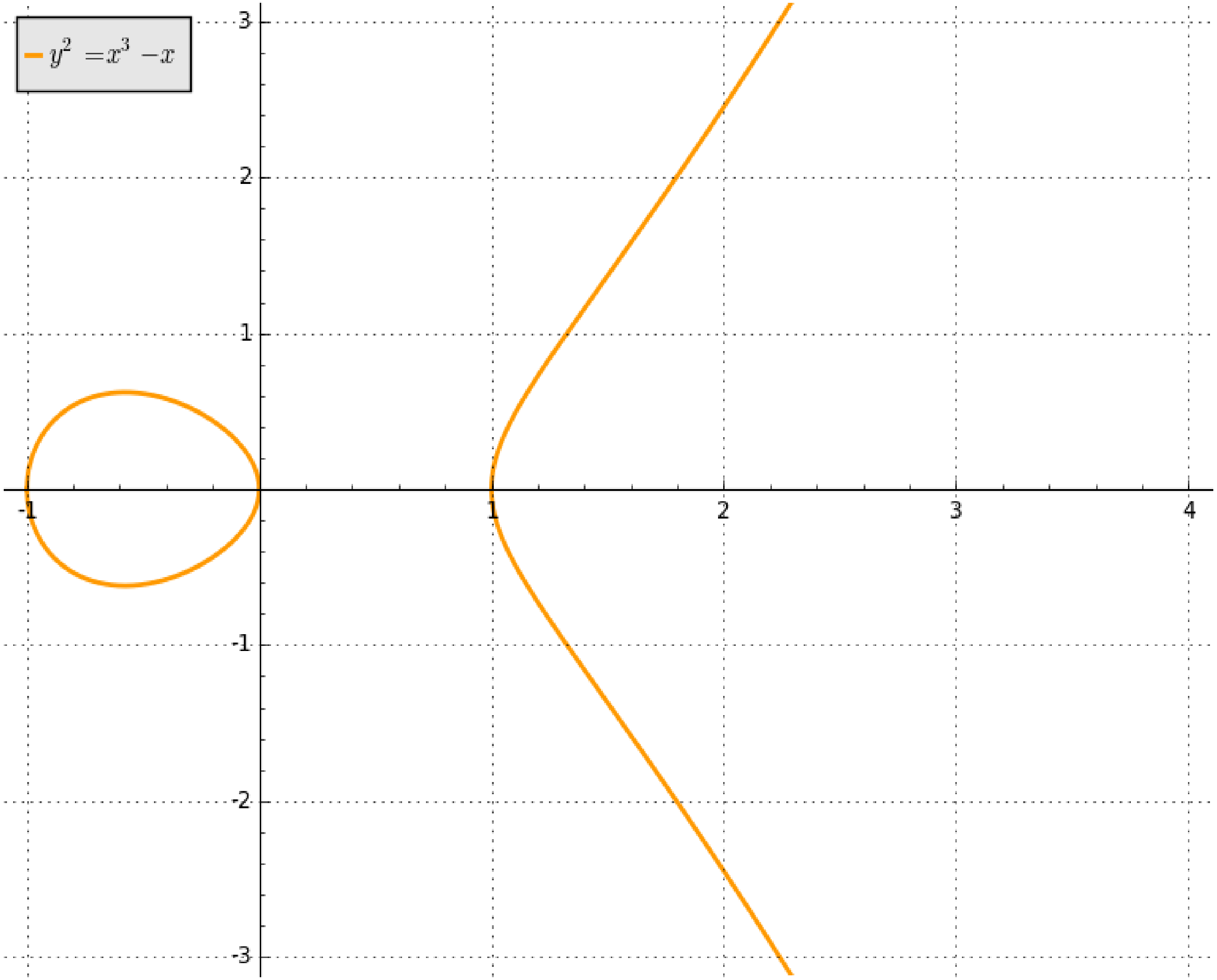
Other equivalent definitions are the following:

- A nonsingular projective genus 1 curve over **K** equipped with a **K**-rational point O
- A one dimensional group variety

Elliptic curves over $K = \mathbb{R}$

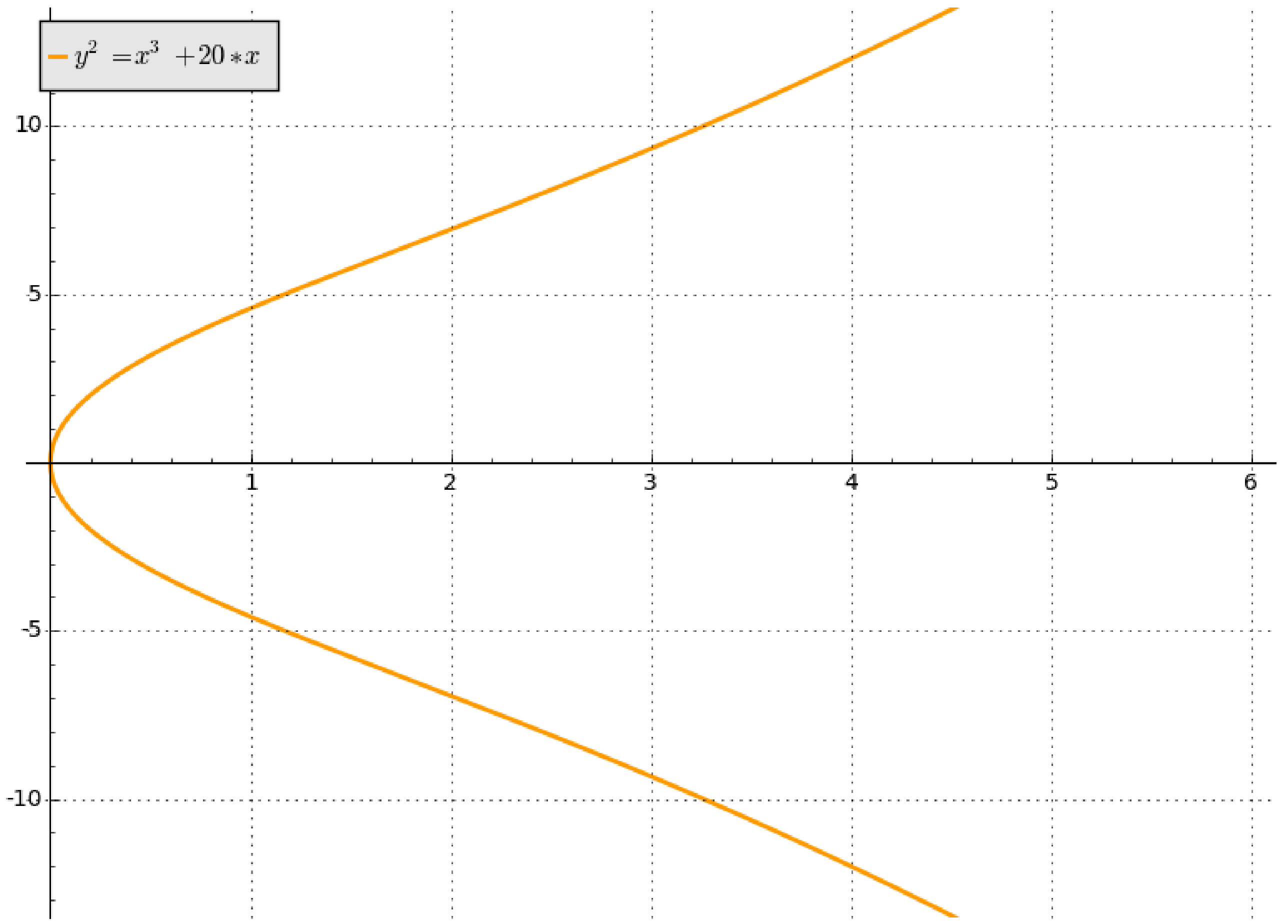
$$y^2 = x^3 - x$$

$$\Delta = 64$$



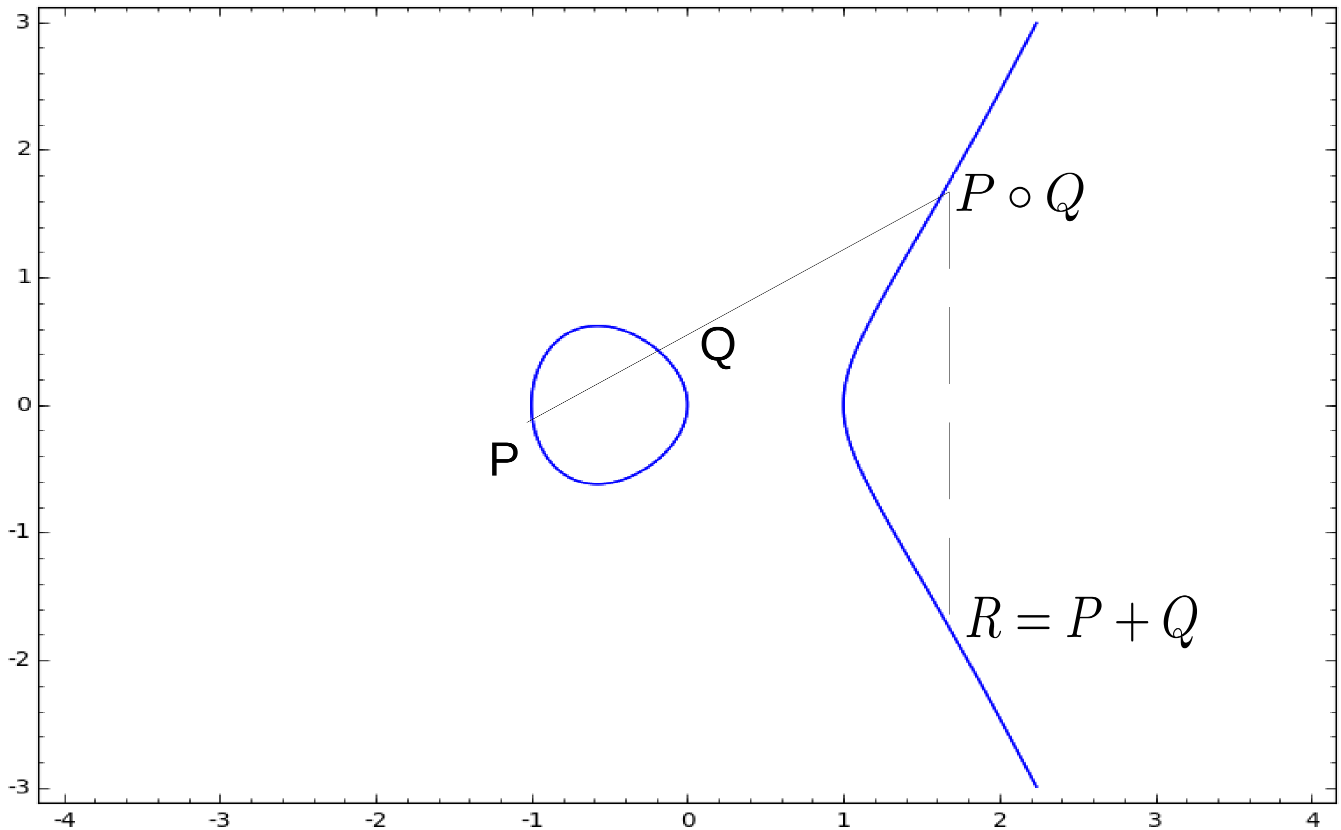
$$y^2 = x^3 + 20x$$

$$\Delta = -512000$$

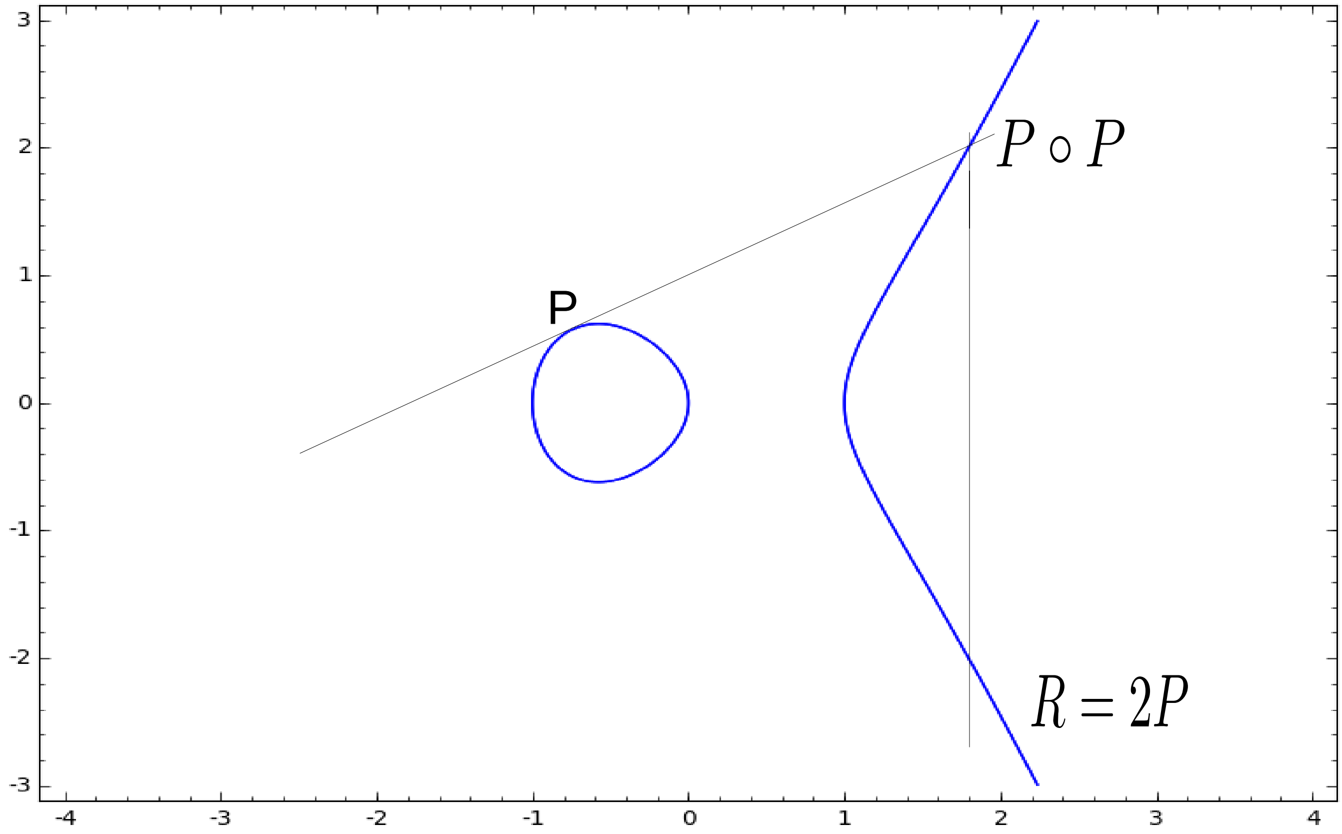


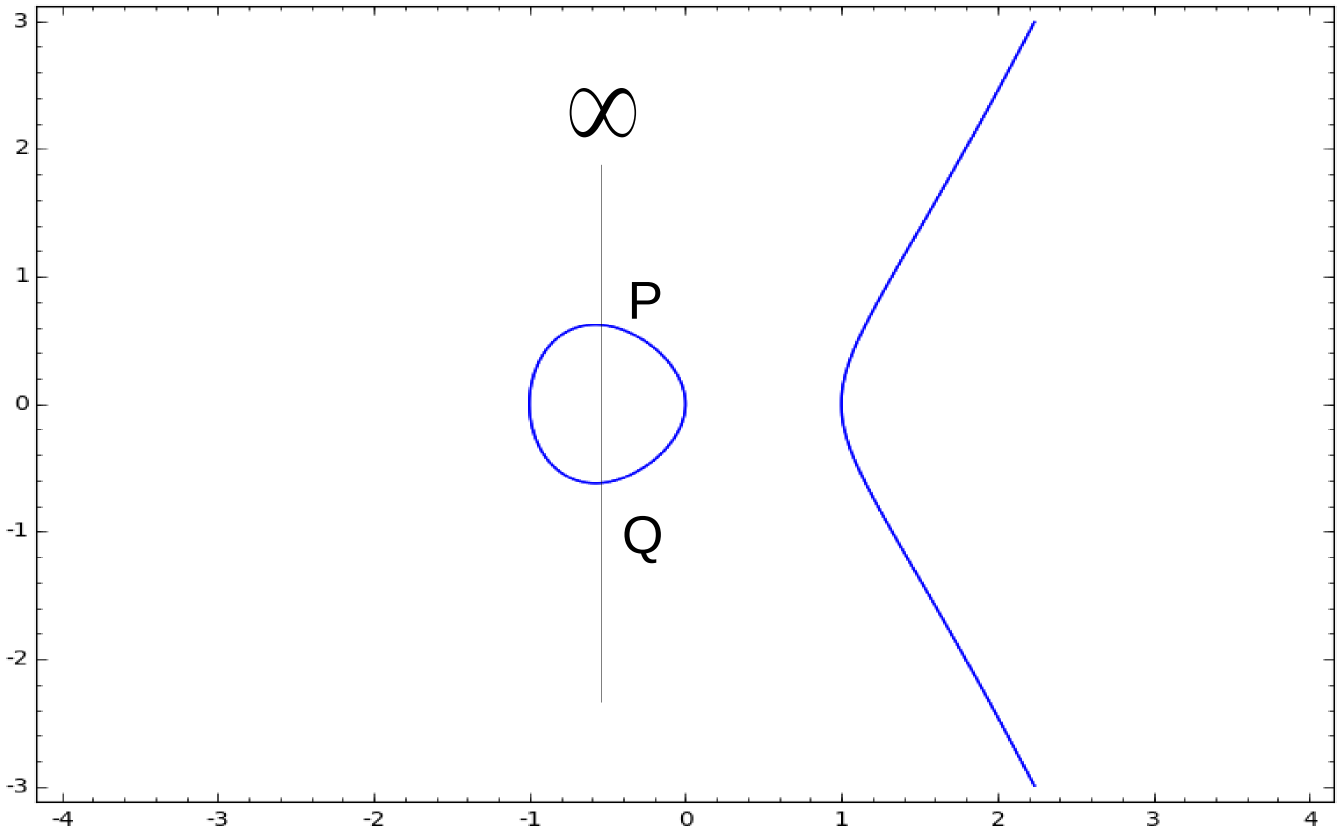
Group Law (chord-tangent method)

We can easily define a group law on an elliptic curve over K, geometrically.



Doubling a point : P+P=R





There is not an extra in the plane that do the job. So the extra point at Infinity is the third point of the line PQ.

The set $E(\mathbf{K})$ (including $\{\infty\}$) with the previous operation is an Abelian group with $\infty \equiv O$ neutral element

$$P + O = O + P = P$$

$$P + Q = Q + P$$

$$P + (-P) = O$$

$$P + (Q + R) = (P + Q) + R$$

The proof is lengthy and uses explicit formulas

How the group E(K) looks like?

This depends on the field K.

$$K = \mathbb{R}$$

- Then we have one or two connected components.

$$E(\mathbb{R}) \cong S^1 \ = \ \{z \in \mathbb{C} : |z| = 1\} \ \ \text{(one real root)}$$

$$E(\mathbb{R}) \cong S^1 \times C_2 \ \ \text{(three real roots)}$$

$$K = \mathbb{C}$$

- Then,

$$E(\mathbb{C}) \cong S^1 \times S^1 \ (torus)$$

$$K = \mathbb{Q}$$

Here we have the result of Mordell proved in 1922.

Theorem (Mordell, 1922)

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{Torsion} \times \mathbb{Z}^r$$

So a point P in E(Q) can be written as

$$P = n_1 P_1 + \cdots + n_r P_r + T,\ T \in E_{Torsion}(\mathbb{Q}),\ n_i \in \mathbb{Z}$$

The free part

- The non negative integer r, is called rank.
- If r=0 then the elliptic curve has finitely many rational points
- If r>0 it has infinitely many rational points

Conjecture. There exist groups E(Q) with arbitrary large rank.

Elkies found an elliptic curve with rank at least 28.

Meaning of the rank

- Is not always easy to compute it
- We don't know if there is an upper bound
- Is used to compute integer points on elliptic curves (Tzanakis-Stroeker)

Birch and Swinnerton-Dyer Conjecture (1960 - 1965)

BSD predicts the value of rank in terms of the L-function attached to E.

$$L(E,s) = \prod_{p \nmid N_E} (1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p \mid N_E} (1 - a_p p^{-s})^{-1}$$

$a_p = 1 + p - |E(\mathbb{F}_p)| \qquad N_E \text{ conductor of E}$

Is convergent for $Re(s) > 3/2$

Hasse, conjectured that L(E,s) can be defined to the whole complex plane.

This was proved, so it makes sense to define order at s=1.

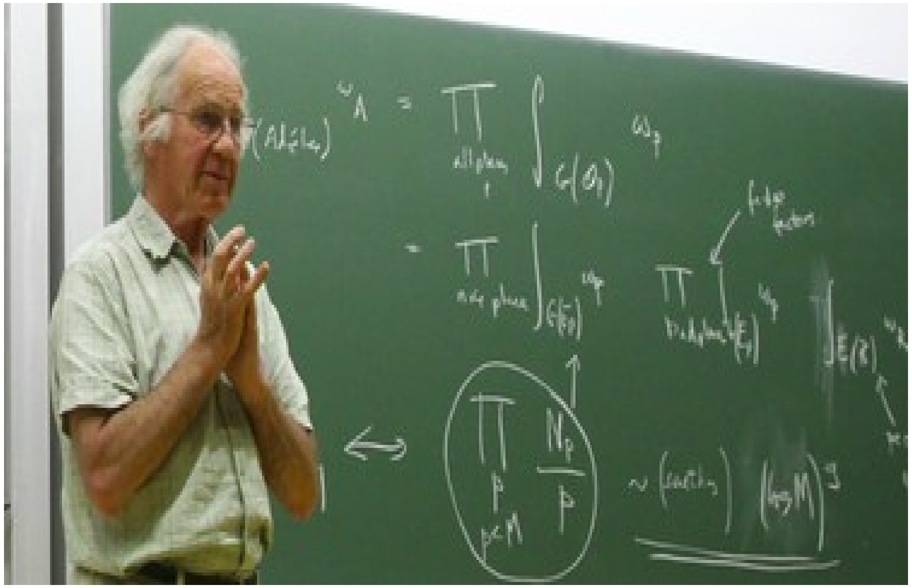
$ord_{s=1} L(E, s) : \text{Analytic rank}$

BSD conjecture asserts that the rank of the elliptic curve is equal to $ord_{s=1} L(E, s)$

BSD, a million dollar problem

BSD. Analytic rank = Geometric rank for E/Q

i.e $$L(E,s) = c(s-1)^r + \sum_{j\geq 1} c_j (s-1)^{j+r},\ c \neq 0$$



Bryan Birch

Peter Swinnerton-Dyer

In 2015 Bhargava & Shankar, proved that a positive proportion of elliptic curves over Q have analytic rank zero and (from a theorem of Kolyvagin) satisfy BSD.

The torsion part

- $E(\mathbb{Q})_T$ is a finite group. Contains all the rational points of E of finite order.

  Lutz-Nagell Theorem.

  Let $y^2 = x^3 + Ax + B$

  with A,B integers. If $(x_0, y_0) \in E(\mathbb{Q})_T$

  then $x_0, y_0 \in \mathbb{Z}$ and $y_0^2 | 4A^3 + 27B^2$

The torsion part

B. Mazur proved the following.

Theorem (Mazur, 1977).

$$E(\mathbb{Q})_T \cong C_N, \ 1 \leq N \leq 10 \ or \ 12$$

or

$$E(\mathbb{Q})_T \cong C_N \times C_{2N}, \ 1 \leq N \leq 4$$

$\mathit{The\ Set}\ E(\mathbb{Z})$

Theorem (Siegel, 1928). For

$$E : y^2 = x^3 + Ax + B,\ \ A, B \in \mathbb{Z}$$

we have $|E(\mathbb{Z})| < \infty$

In fact Siegel proved the following stronger theorem

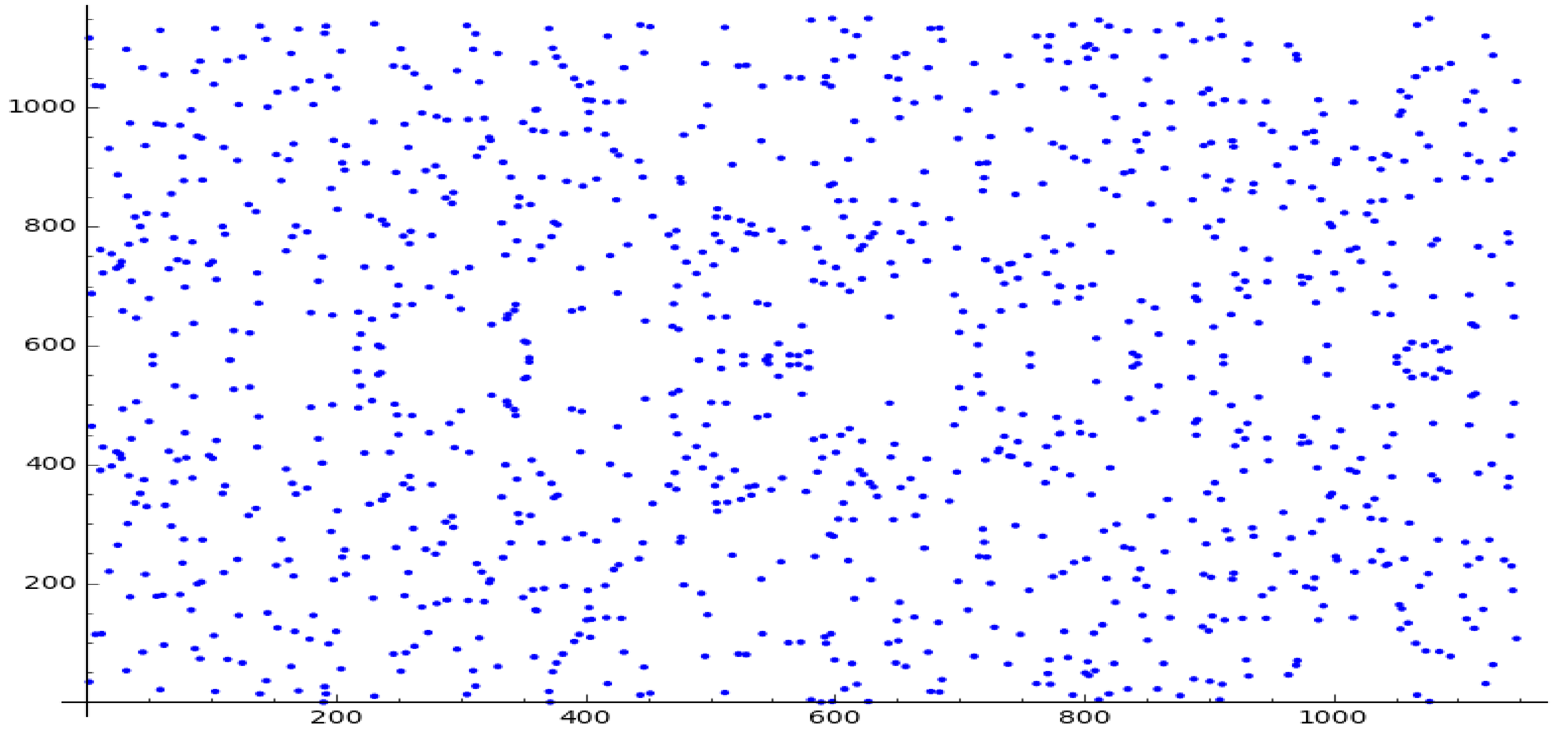
Theorem (Siegel) If $P \in E(\mathbb{Q})$ and $x(P) = \dfrac{a(P)}{b(P)}$

$$\lim_{P \in E(\mathbb{Q}), \max(|a(P)|, |b(P)|) \to \infty} \frac{\log |a(P)|}{\log |b(P)|} = 1$$

$$K = \mathbb{F}_q$$

In this case the set $E(\mathbb{F}_q)$ is finite. The computation of $|E(\mathbb{F}_q)|$ is crucial in the development of Elliptic Curve Cryptography (ECC).

An example



$$p = 1151 \quad y^2 = x^3 - x - 1$$

$$E(\mathbb{F}_p) \cong \mathbb{Z}/560\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

Theorem (Hasse, 1936). Let q be a prime or a prime power. Then,

$$|q+1-\#E(\mathbb{F}_q)| \leq 2\sqrt{q}$$

So $\#E(\mathbb{F}_q) = q + 1 - \beta, \quad |\beta| \leq 2\sqrt{q}$

A result of Waterhouse tell us that for every β with $|\beta| \leq 2\sqrt{q}$ there is an elliptic curve with order $\#E(\mathbb{F}_q) = q + 1 - \beta.$

The theorem gives us the values of β in relation with q.

Order of $E(\mathbb{F}_q)$

A simple way to compute the order of the set $E(\mathbb{F}_q)$

for small **prime** q=p, is by using brute force.

For x=0,1,,...,p-1, we check if $x^3 + Ax + B$

is quadratic residue modp. This method demands $O(p \log p)$ bit-operations.

This method is practical for primes $p \approx 2^{30}$

There is an improvement $O(p^{1/4})$

(but is still exponential).

In 1995 Schoof managed to find a polynomial time complexity algorithm for computing the order of an elliptic curve over a prime finite field. The bit-complexity is $O((\log p)^6)$

Elkies and Atkin further improve it.

Order of a point P

Definition

Let P be a point of an elliptic curve over a field K, we define the order of the point P to be the cardinality of subgroup generated by the point P. That is

$$ord(P) = |\langle P \rangle|$$

The group of order m, E[m]

- With E[m] we denote all the points of order m of an elliptic curve E/K.

$$E[m] = \{P \in E(\overline{K}) : mP = O\}$$

Theorem (group structure of E[m])

Let q be a prime p or a power of p.

If $\gcd(p, m) = 1$ then $E[m] \cong \mathbb{Z}_m \times \mathbb{Z}_m$

If $m = p^r m', \; \gcd(p, m') = 1$

then $E[m] \cong \mathbb{Z}_m \times \mathbb{Z}_{m'}$,

or $E[m] \cong \mathbb{Z}_{m'} \times \mathbb{Z}_{m'}$

The Group structure of the elliptic curve over a finite field

Theorem. $E(\mathbb{F}_q) \cong \mathbb{Z}_n \times \mathbb{Z}_{cn}, \text{ where } c \geq 0$

If c>0, then $n|q-1$

Example

Consider the curve $E: y^2 = x^3 + 7$

over the finite field $\mathbb{F}_{13}$

Then, $E(\mathbb{F}_{13}) \cong \mathbb{Z}_7$.

is cyclic.

DLP over a Group

Let G be a multiplicative group.

- **Discrete Logarithm Problem over G.**

Input : Let g in G and $a \in \langle g \rangle$

and ord(g) = n.

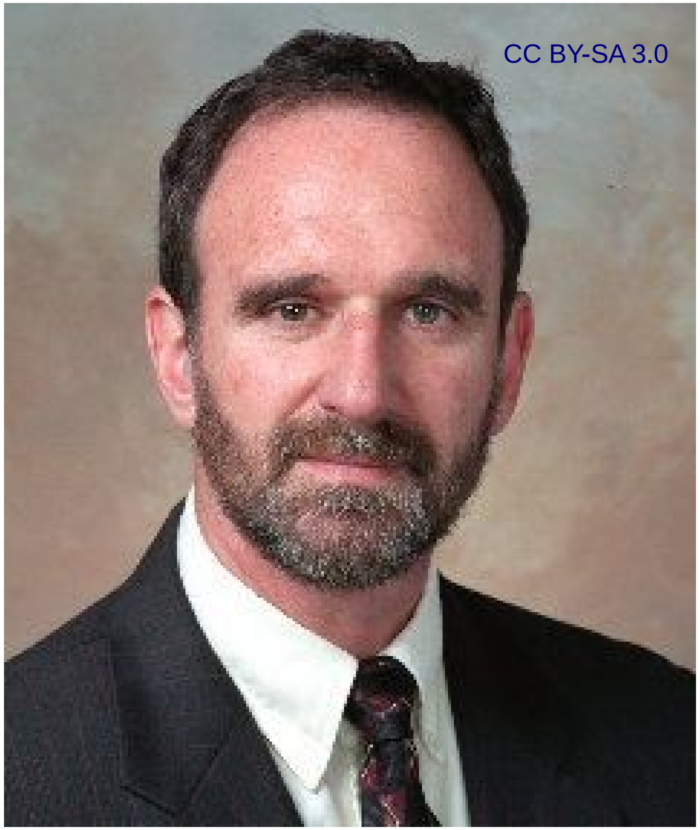
Output : Find k such that $g^k = a$

k is determined uniquely modn

If G is additive

find k such that $k \cdot g = a$

Diffie-Hellman protocol



Martin Hellman

Whit Diffie

Providing this protocol Diffie and Hellman solved the problem of key exchange.

They used DLP in the group $\mathbb{Z}_p^*$

The world’s most famous cryptographic couple, *Alice and Bob* want to exchange a key

ALICE

$b \xleftarrow{\$} \mathbb{Z}_p^*$

Send a prime p and
a number 0<g <p

$\longrightarrow$

$\longleftarrow$

$$g^a \mod p$$

$\longrightarrow$

$$g^b \mod p$$

BOB

$a \xleftarrow{\$} \mathbb{Z}_p^*$

Alice computes $(g^a)^b$

Bob computes $(g^b)^a$

Eve, an eavesdropper, has the pair (g^a, g^b)

and she wants to compute g^{ab}

A function that does such a computation is called Diffie-Hellman function.

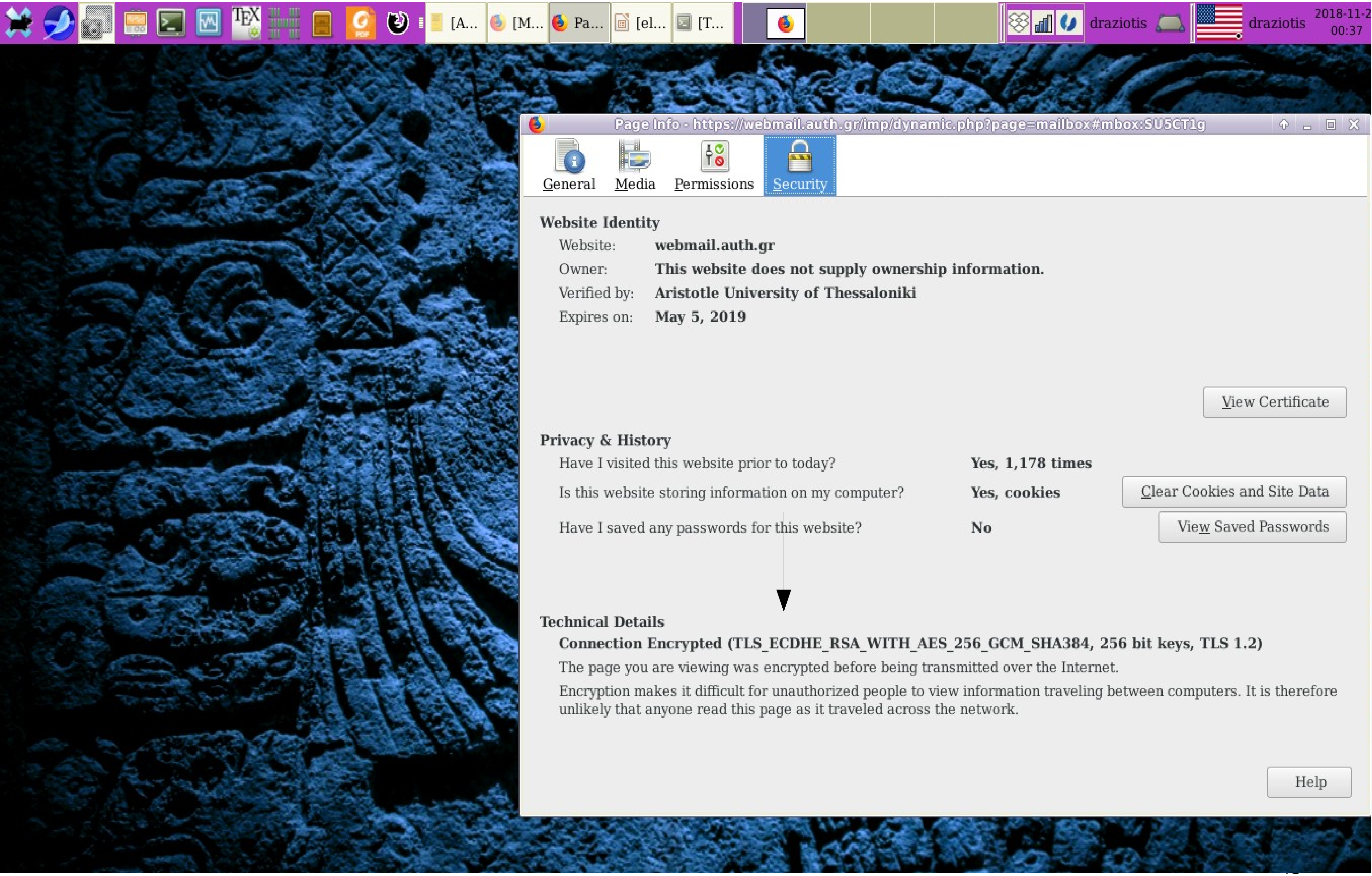
$$DH(g^a, g^b) = g^{ab}$$

One way to compute this is by using the DLP.

The inverse, i.e. if the computation of DH, solves DLP, is an open problem (**Diffie-Hellman** problem)

If we substitute the group of integers modulo p, with a group of an elliptic curve over a finite field, we get the Elliptic Curve variant of Diffie-Hellman (ECDH). This, protocol is used from many TLS-servers.

- For instance from Aristolte University of Thessaloniki (Webmail server).



[A...
[M...
Pa...
[el...
[T...
draziotis
draziotis
2018-11-2
00:37
Page Info - https://webmail.auth.gr/imp/dynamic.php?page=mailbox#mbox:SU5CT1g
General
Media
Permissions
Security
Website Identity
Website: webmail.auth.gr
Owner: This website does not supply ownership information.
Verified by: Aristotle University of Thessaloniki
Expires on: May 5, 2019
View Certificate
Privacy & History
Have I visited this website prior to today? Yes, 1,178 times
Is this website storing information on my computer? Yes, cookies
Clear Cookies and Site Data
Have I saved any passwords for this website? No
View Saved Passwords
Technical Details
Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256 bit keys, TLS 1.2)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.
Help

Also Bitcoin protocol uses ECC

Bitcoin uses the elliptic curve $y^2 = x^3 + 7$

over the finite field with p elements, where

$p = 2^{256} - 2^{32} - 977$

which provides about 128-bit security (according to Pollard rho algorithm).

ECC

- In 1985, Koblitz and Miller independently discover the ECC.
- Although, the first application of elliptic curves in cryptography was H.Lenstra factorization algorithm (1984).
- Further, S. Goldwasser and J. Kilian in 1986, and Atkin (the same year) provided a primality test using elliptic curves.

ECDLP

The problem of elliptic curves that we use in cryptography is the **Discrete Logarithm Problem (ECDLP).**

Let P be a point of an elliptic curve over a finite field and

$$G = \langle P \rangle = \{nP : n \in \mathbb{Z}\}$$

be the subgroup generated by this point. Let Q be in G. Then, we want to find an integer k, such that

$$Q = kP, \ (k = \log_P(Q))$$

The morphism $\log_P : G \to \mathbb{Z}/N\mathbb{Z}$

where N=|G| is isomorphism.

The inverse map $\phi : \mathbb{Z}/N\mathbb{Z} \to G$

is $\phi(k) = kP$

An example

We consider the elliptic curve

$$y^2 = x^3 + 10x + 17$$

In this case we can prove that

$$E(\mathbb{F}_{331}) \cong \mathbb{Z}_{335}$$

We consider the following points

$$P = (303, 151),\ Q = (326, 175)$$

We can check that both points generate $E(\mathbb{F}_{331})$

We want to compute $N = \mathrm{dlog}_P(Q)$

i.e. $Q = N \cdot P$

Not only exchanging messages with elliptic curves

- As we saw we can use elliptic curves to exchange keys using the DH protocol
- Also, using El Gamal protocol we can use elliptic curves to send encrypted messages
- And finally, using DSA with elliptic curves, we can sign messages

Attacks to DLP in a group G

- Shank's Algorithm (baby steps-giant steps)
- Pollard Rho
- Pohlig-Hellman (applied, when the order of the group is a smooth integer)

Attacks in the multiplicative group modulo p

- Index calculus method

  has subexponential complexity (best algorithm today)
- First developed in 1920 by Kraitchik (for prime fields)
- The index calculus does not seem to work for Elliptic curves. So, ECDLP provides smaller keys than RSA, classical DH for the same level of security.
- Although, Silverman in 1998 circulated an outline of an attack called xedni. Time analysis showed that it takes super-polynomial time to compute discrete logs.

Pairing based cryptography

- In 2001 proposed by D. Boneh, M. Franklin and others.

  They answered an old question of Adi Shamir :

  find an efficient pk cryptosystem where the public key's of Alice *are her identity.*
- Short signatures schemes, Boneh,Lynn,Shacham
- Also, A. Joux using pairings manage to solve the tripartite DH problem.
- Further, pairings were used to attack ECDLP

Pairings

- The Weil pairing over an elliptic curve $E/\mathbb{F}_q$ is a map

  $e_N : E[N] \times E[N] \to \mu_N = \{x \in \overline{\mathbb{F}}_q : x^N = 1\}$
  $\gcd(N, p) = 1.\ p = char(\mathbb{F}_q)$

  Which has the following properties

  $e_N(S_1 + S_2, T) = e_N(S_1, T)e_N(S_2, T)$
  $e_N(S, T_1 + T_2) = e_N(S, T_1)e_N(S, T_2)$
  $e_N(T, T) = 1$

** This is not the definition

- Miller's algorithm allows us to compute in linear time the values of a Weil pairing. This is the reason we apply pairing in cryptography.

Using pairings to solve ECDLP

- MOV attack.

  They managed to reduce the ECDLP to a classical DLP problem, over a finite field.

- A. Menezes, T. Okamoto and S. Vanstone (1993) showed that one can reduce the ECDLP for a supersingular elliptic curve over a finite field $\mathbb{F}_q$ to a classical DLP in $\mathbb{F}^*_{q^d}, \ (d \leq 6)$
- Supersingular elliptic curves are those

  where $\#E(\mathbb{E}_q) \equiv 1 \pmod{p}$

- If $p \geq 5$

  $E/\mathbb{F}_p$ is supersingular if-f $\#E(\mathbb{F}_p) = p + 1$

The idea of MOV attack

Let $P = aQ$

Find a point R in E such that

$$z = e_N(P, R) \neq 1$$

Then, from properties of the Weil pairing

$$e_N(Q, R) = e_N(aP, R) = e_N(P, R)^a = z^a$$

in the group $\mu_N \subset \mathbb{F}_{q^d}^*$

If d is small we can apply algorithms for solving DLP.

d is called **embedding degree** and is the smallest k such that

$$\mu_N \subset \mathbb{F}_{q^d}^*$$

- Other curves where ECDLP is easy are the anomalous curves, i.e. curves where $\#E(\mathbb{F}_p) = p$

Quantum attacks to ECDLP

Peter Shor discovered a polynomial time (probabilistic) algorithm that solves DLP (and factorization problem, too) in a generic group G.

So, if a quantum computer constructed in the future ECDLP is not secure (and all the modern Public crypto, too).

This algorithm needs

$$O(\log_2 N(\log_2 \log_2 N)(\log_2 \log_2 \log_2 N))$$

quantum gates.

Quantum resistant ECC

- Elliptic curves again provides a solution.

  The problem of finding isogenies over superelliptic curves

  is quantum resistant.
- Based on the previous problem we can define a **S**upersingular **I**sogeny **D**iffie–**H**ellman key exchange (SIDH).
- The proposed protocol uses 2688-bit public keys for 128-bit security.
- Further, provides forward secrecy, i.e. protects past sessions against future compromises of secret keys or passwords.

SIDH

- The set of isogenies of a supersingular elliptic curve together with operation of composition form a non-abelian group.
- The security of SIDH is closely related to the problem of finding the isogeny mapping between two supersingular elliptic curves with the same number of points.

A map $\phi : E_1 \to E_2$ is called isogeny over $\mathbb{F}_q$ if it is a rational map and a group homomorphism.

- Andrew Childs, David Jao, and Vladimir Soukharev, provided a subexponential **quantum** of attack for isogeny problem for elliptic curves (2010).
- This applies to ordinary elliptic curves

References

[1] *Andrea Enge*, Elliptic curves and their application to cryptography (Springer 1999).

[2] *S. Galbraith*, Public key cryptography, Cambridge University Press

[3] *A.H. Koblitz, N. Koblitz, A. and Menezes,* Elliptic curve cryptography : The serpentine course of a paradigm shift

[4] *J.H. Silverman*, The arithmetic of Elliptic curves, Springer

[5] *J.H. Silverman*, Talk, “The Ubiquity of Elliptic Curves”

Thank you!