Lecture 6: Elliptic curves. PKI. Zero-knowledge proofs

Course instructors: Alexey Frolov and Yury Yanovich

Teaching assistant: Stanislav Kruglik

Techical assistants: Marina Dudina, Anton Glebov, Evgeny Marshakov

November 15, 2018

Problem

RSA – factorization of big numbers

ElGamal – discrete logarithm

There are sub-exponential algorithm to decrypt ElGamal and RSA

Solution

Cryptography on elliptic curves

Why elliptic curves?

- No sub-exponential algorithms
- Fast on chip and program realization
- Give an ability to use previously developed cryptography schemes because group of points in elliptic curve is an algebraic group

What is it?

Elliptic curve E over the field F can be defined by equation that connect x and y coordinates of curve E:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Elliptic curve can be presented in a canonic Wierstrass form (if char F $\neq 2, 3$):

$$y^2 = x^3 + ax + b$$
$$y^2 = x^3 - px - q$$

What is it?

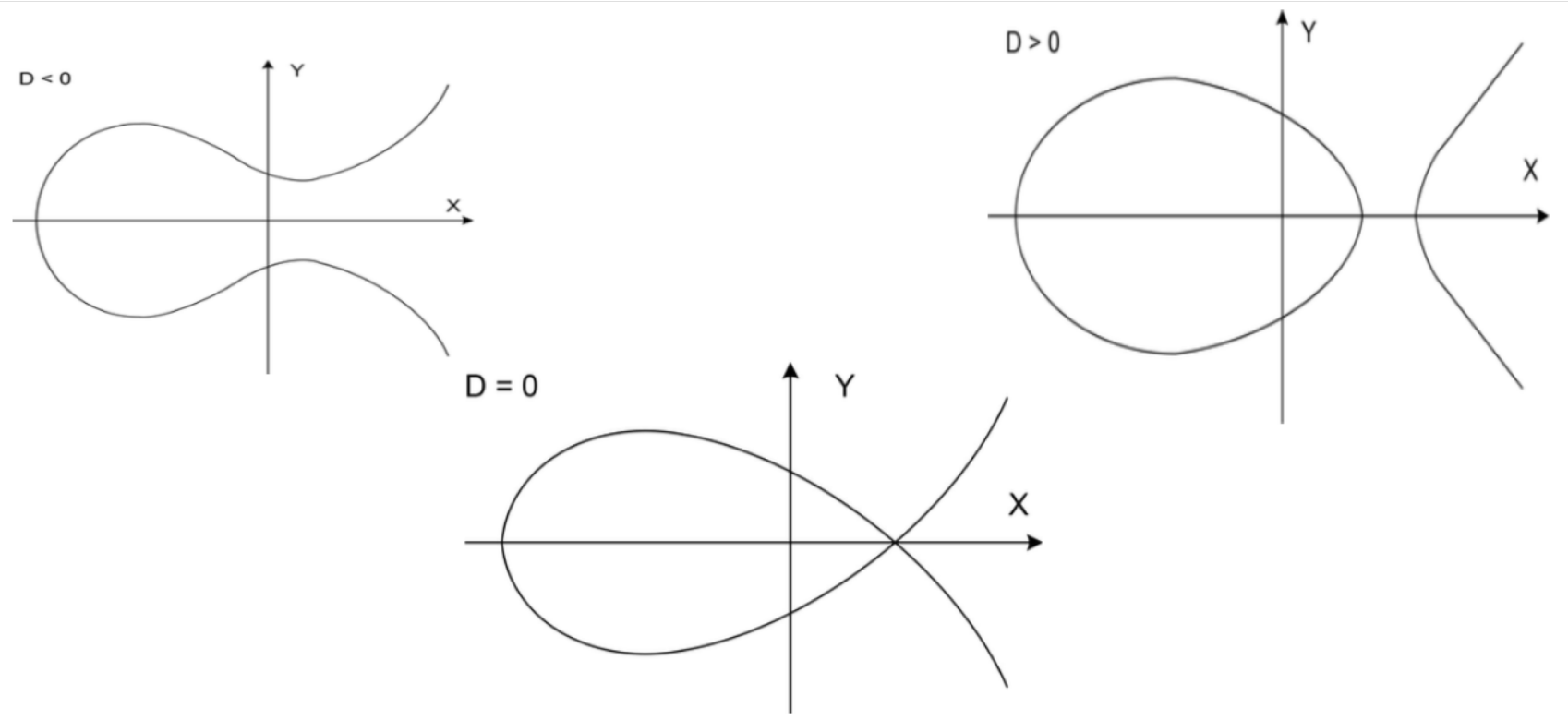
On elliptic curve in Wierstrass form we can determine invariant

$$J(E) = 1728\frac{4a^3}{4a^3 + 27b^2}$$

Also this elliptic curve has a determinant D. Let x_1, x_2, x_3 be the roots of equation $x^3 + ax + b = 0$

$$D = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2 = -16(4a^3 + 27b^2)$$

Types of curves for different values of D



Algebraic group of points of elliptic curve

(x,y) – element of the group

“0” – infinite point

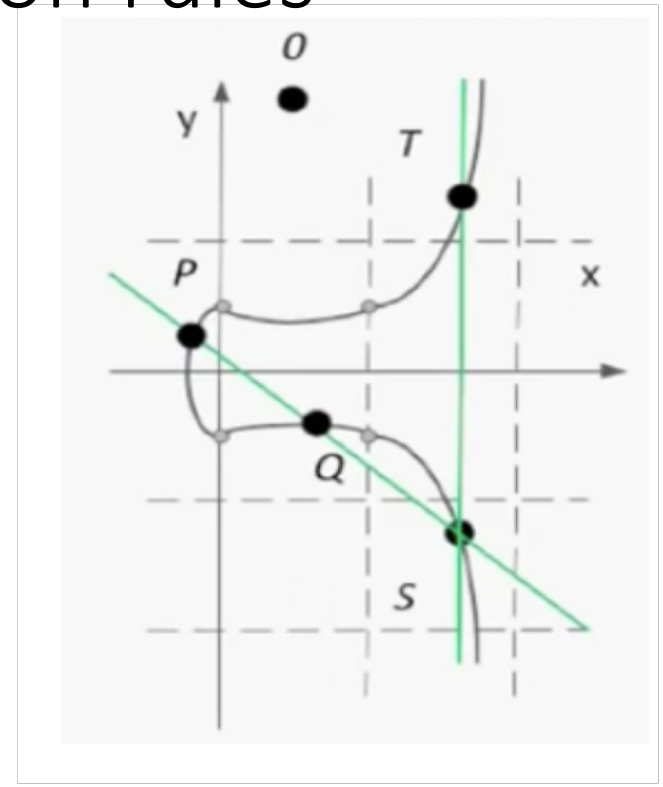
Group operation: T=P+Q

P+Q+R=0

R=-T

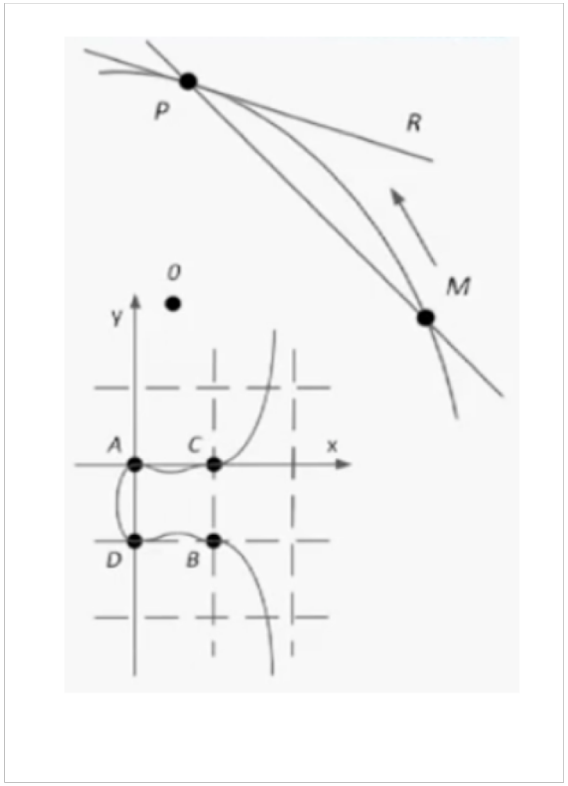
Inverted element by group operation is the element symmetric by oX

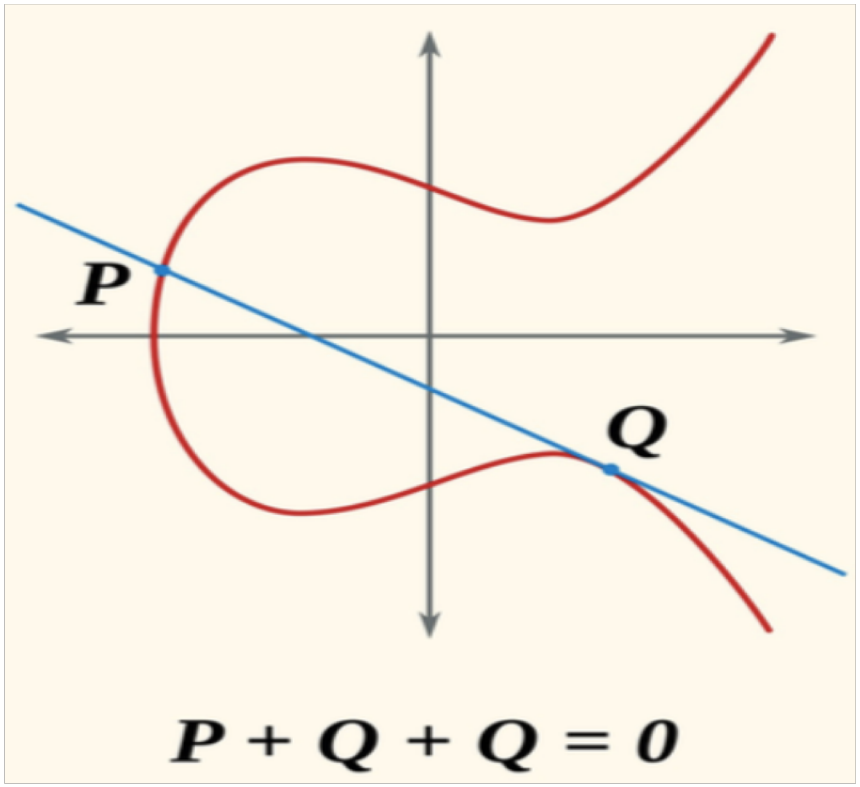
Group operation rules

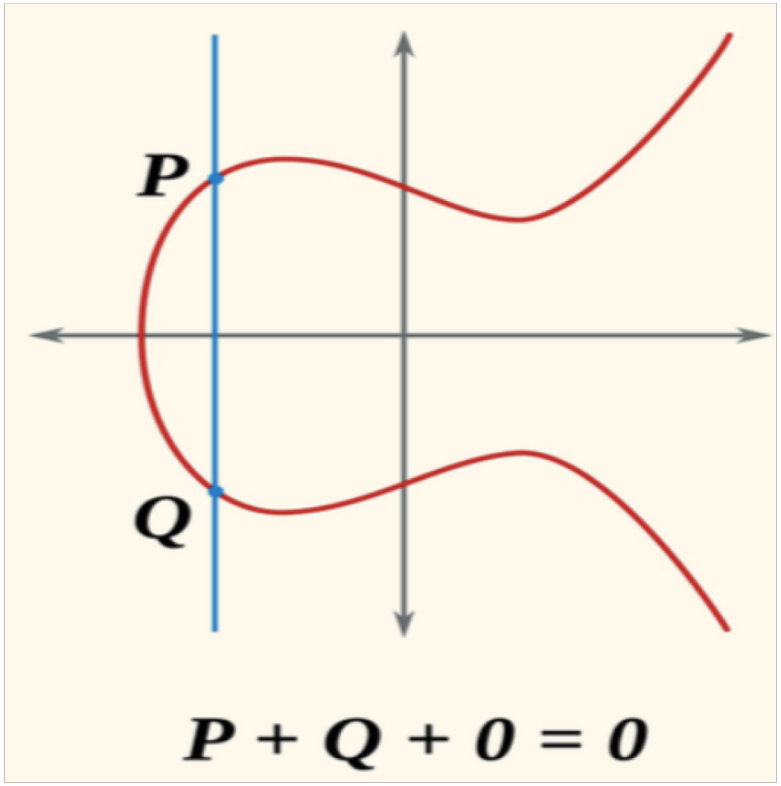


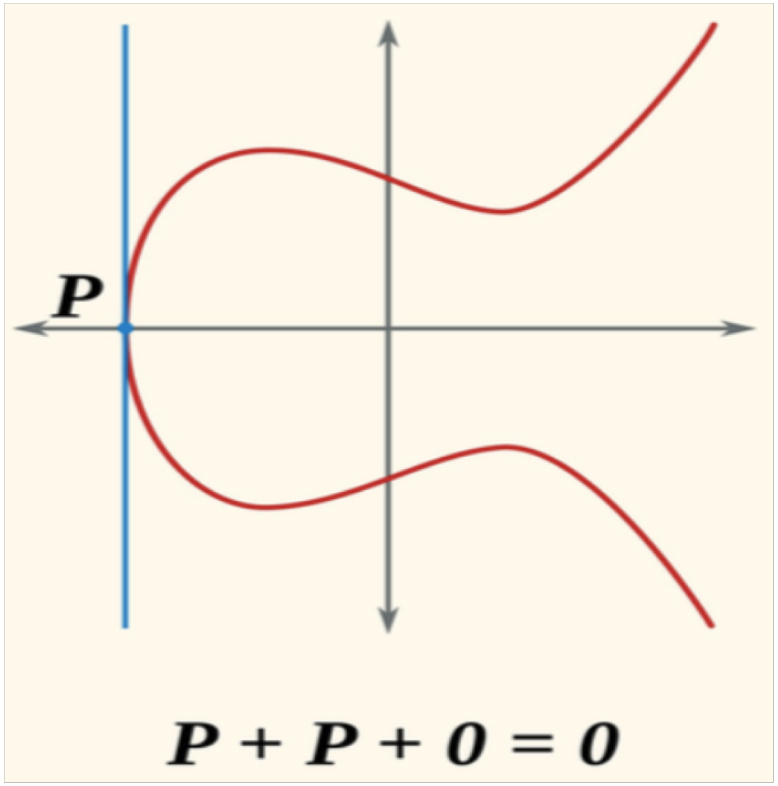
R+Q+S=0

Group operation rules




P
Q
P + Q + Q = 0


P
Q
P + Q + 0 = 0


P
P + P + 0 = 0

Group operation in analytical form

- Let us know $P(x_p, y_p)$ and $Q(x_Q, y_Q)$
- We want to find $R = (x_R, y_R)$ s.t. P+Q+R=0

or

- We want to find $T = (x_T, y_T)$ s.t. P+Q=T

Different formulas for different cases of points placement!

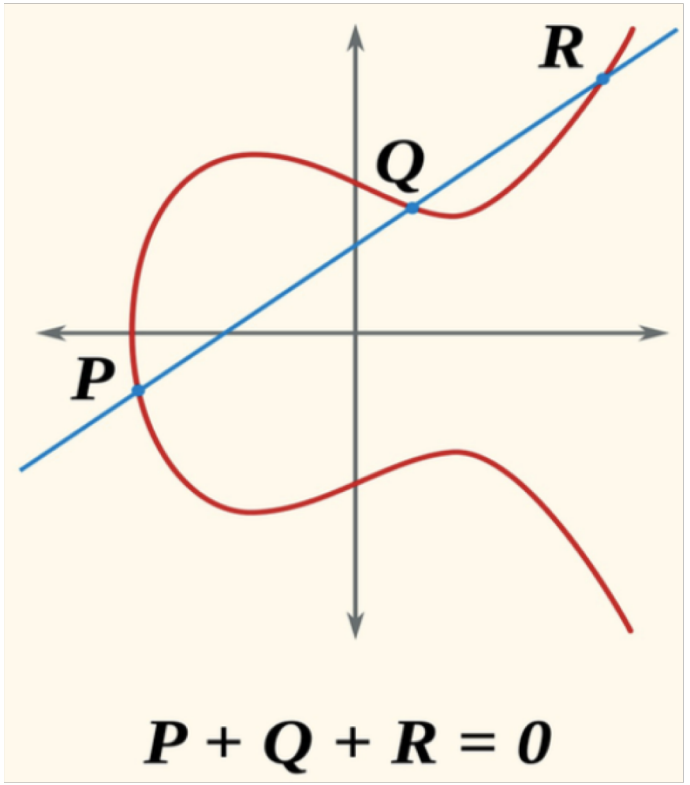
$$s = \frac{y_P - y_Q}{x_p - x_Q}$$

$$x_T = s^2 - x_P - x_Q$$

$$y_T = -y_P + s(x_P - x_T)$$

$$x_R = s^2 - x_p - x_Q$$

$$y_R = y_P - s(x_p - x_R)$$



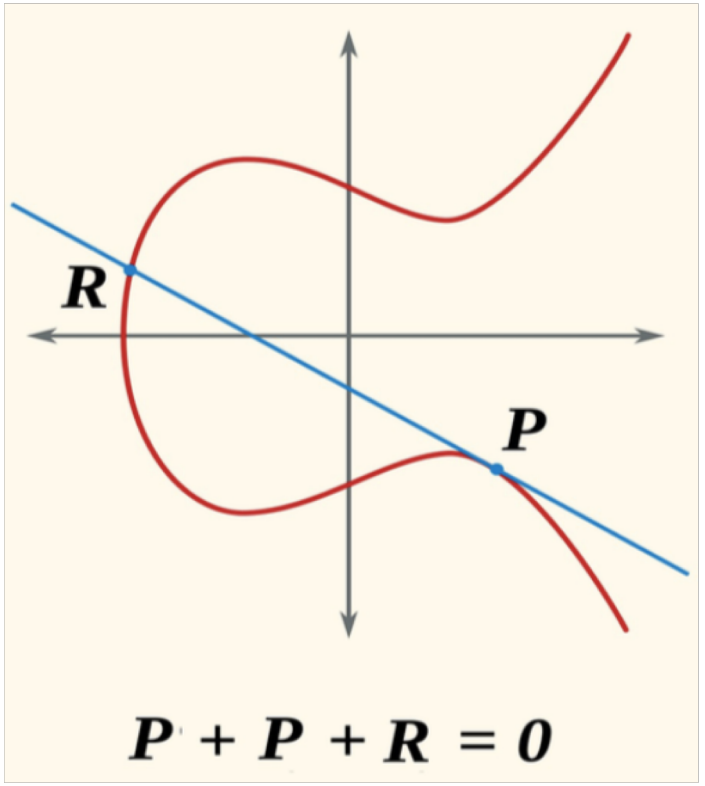
$$s = \frac{3x^2 + a}{2y}$$

$$x_T = s^2 - x_P - x_Q$$

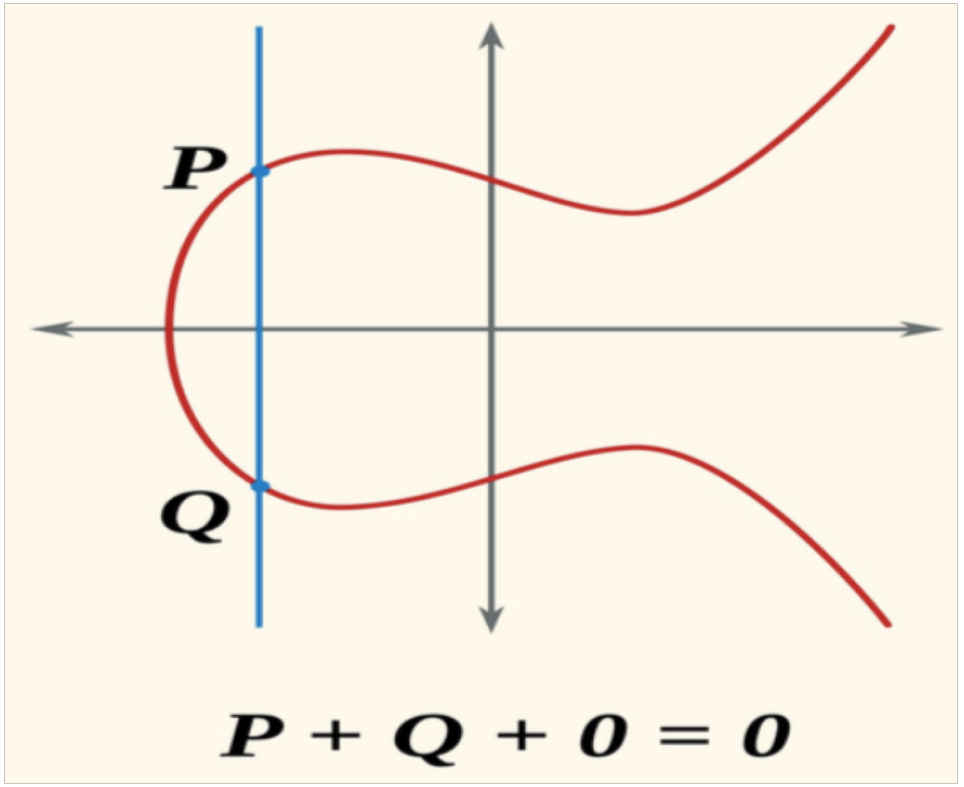
$$y_T = -y_P + s(x_P - x_T)$$

$$x_R = s^2 - x_P - x_Q$$

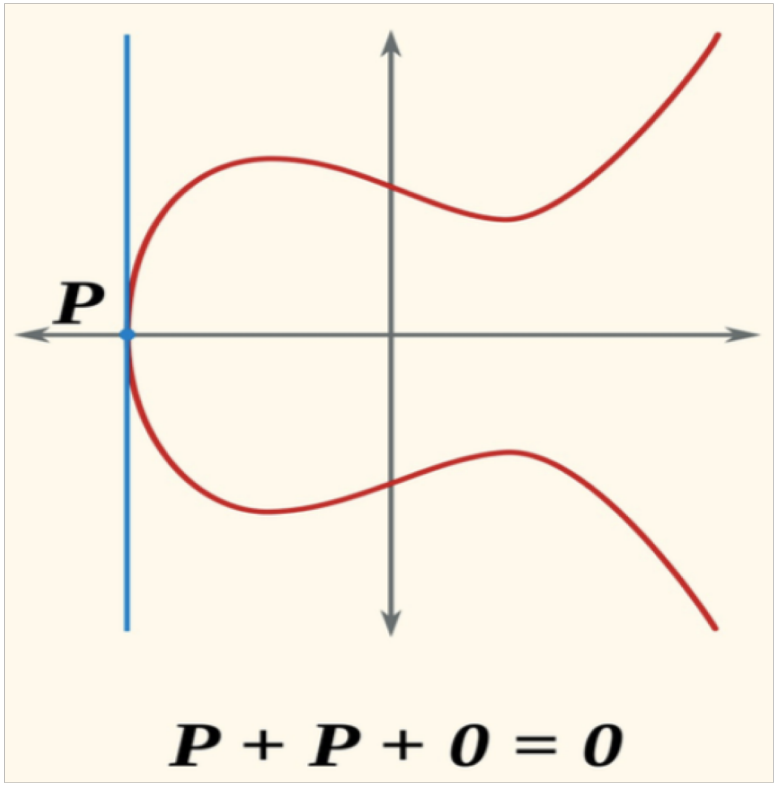
$$y_R = y_P - s(x_P - x_R)$$



T=R=”0”



T=R=”0”



Elliptic curves over finite fields

- All coefficients of elliptic curve are belong to the field
- All operations are conducted over the corresponding modulo
- d times addition of point to itself – d times multiplication to it
- Cyclic group → can be used in cryptography

Example

G={A,B,C,D,0}

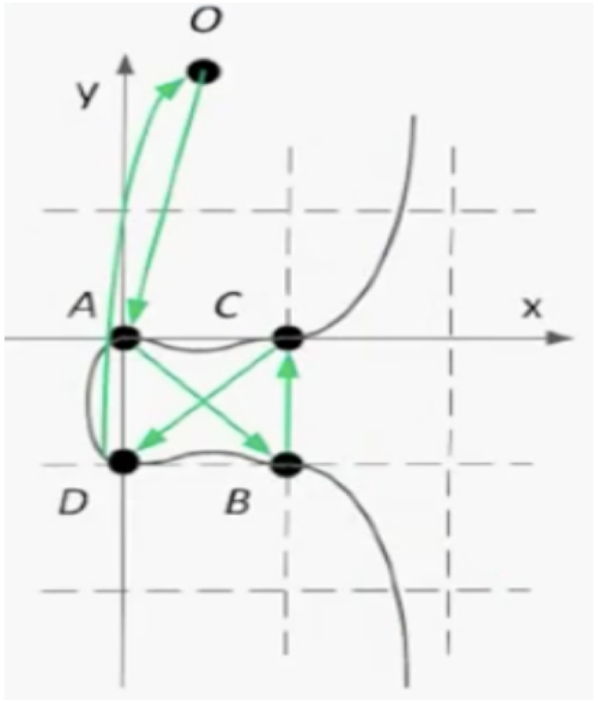
A+A=B

A+B=C

A+C=D

A+D=0

A+0=A



Number of points in group

Hasse's theorem

$$(\sqrt{p} - 1)^2 \leq |E| \leq (\sqrt{p} + 1)^2$$

Subgroup

- Let us take point G of elliptic curve
- By adding point to itself we receive a subgroup with generator G
- Order of group is such number n that $nG ='' 0''$

One-way operation

- ElGamal

$y = g^x mod\ p$

- Elliptic curve cryptography

$Y = xG = G + \cdots + G\ (x\ times)$

Cryptography on elliptic curves

Other things are the same with ElGamal cryptography!

Elliptic curve digital signature (GOST R 34.10-2012)

$p > 2^{255}$ – elliptic curve modulo
G – cyclic subgroup generator
$2^{254} < n < 2^{256}$ – order of cyclic subgroup
E: $y^2 = x^3 + ax + b$

$Q = dG$ ← open (public) key
$0 < d < n$ ← secret (private) key

Sign(private key, m)

- Choose arbitrary k s.t. 0<k<n
- Find C=kG
- If $x_C = 0 \; mod$ p then choose another k

$\sigma = (x_c, s = x_c d + km) \; mod \; p$

Verify (public key, m, σ)

- Find $v = m^{-1} mod\ p$
- s= $x_c d + km$
- Compute $D = (sv)G + (-x_c v)Q$

$x_c = x_D$

Problem of generating common secret key

Problem

If the sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received.

If they use a cipher, they will need appropriate keys.

Blom’s key exchange scheme

Blom's scheme is a symmetric threshold key exchange protocol in cryptography. The scheme was proposed by the Swedish cryptographer Rolf Blom in a series of articles in the early 1980s.

A trusted party gives each participant a secret key and a public identifier, which enables any two participants to independently create a shared key for communicating. However, if an attacker can compromise the keys of at least k users, they can break the scheme and reconstruct every shared key

The trusted party chooses a random and secret symmetric matrix $D_{k,k}$ over finite field GF(p), where p is a prime number.

Each user has it's identifier i

Users secret key g can be computed as $D_{k,k}i$

Now common key can be computed as $g_A^T i_{\mathrm{B}}$ or $g_B^T i_{\mathrm{A}}$

Public key infrastructure

Problem

- Reliable distribution of public-keys is critical otherwise, an intruder can substitute a different public key resulting in disclosing of encrypted contents to unintended parties
- Easier for small groups of cooperating parties
- A public-key certificate system where a certification authority issue certificates for the holders of key pairs

Man-in-the-middle attack

- Let A have a public key P_A
- Let B have a public key P_B

- Are they sure, that P_A and P_B indeed belong to A and B.

Certificate trust

The primary benefits of the certificate system

- one can reliably obtain a large number of parties starting with the knowledge of one party's public-key
- scalability

How to acquire public key of the issuer to verify signature

Whether or not to trust certificates signed by the issuer for this subject

Certification paths

One certificate authority to issue certificates for all!

- Key distribution problem is solved
- is it feasible?

Need multiple certification authorities

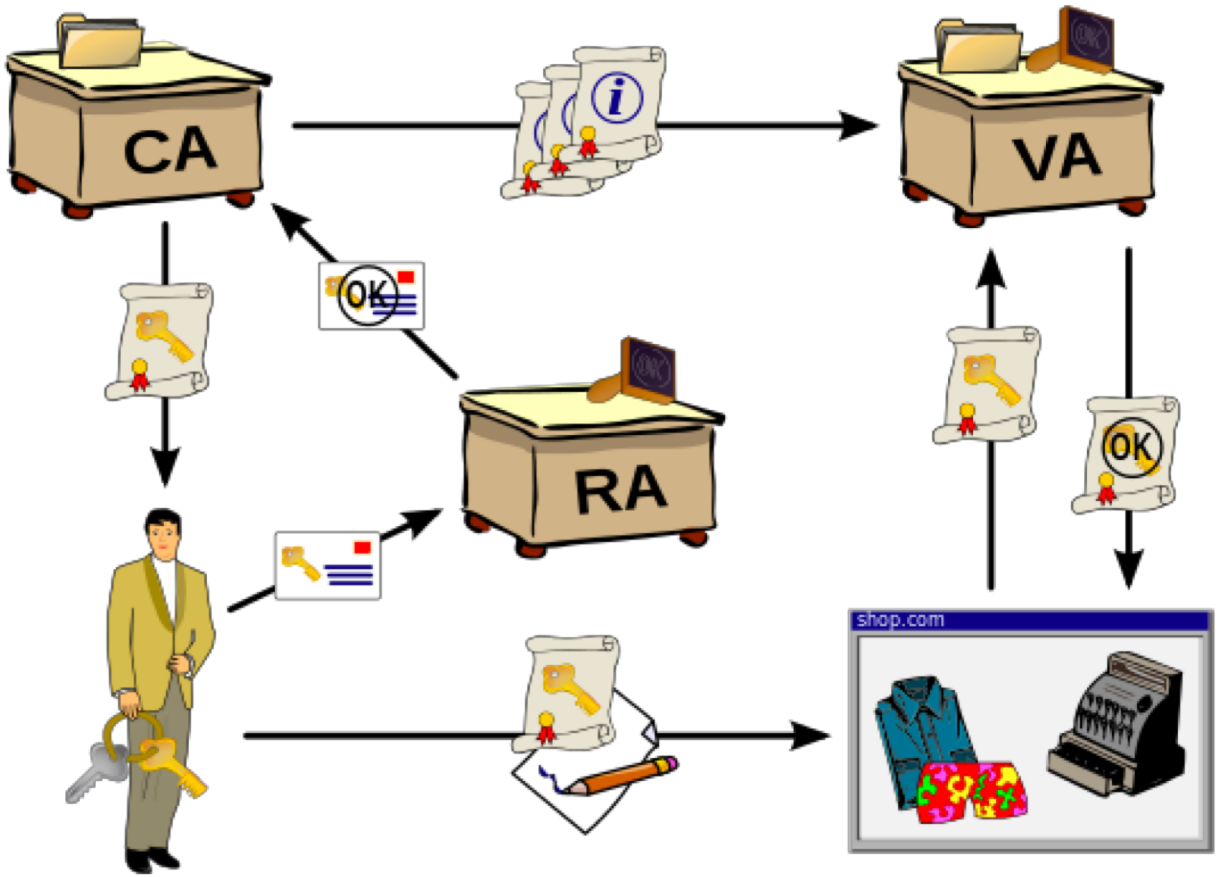
Not practical for a public-key user to have the public-keys of all CAs

The certificate paradigm can be applied recursively to obtain the public keys of a progressively larger number of CAs

- called certificate chain or certificate path

PKI

A PKI consists of:
•A **certificate authority (CA)** that stores, issues and signs the digital certificates
•A ***registration authority*** which verifies the identity of entities requesting their digital certificates to be stored at the CA
•A ***central directory***—i.e., a secure location in which to store and index keys
•A ***certificate management system*** managing things like the access to stored certificates or the delivery of the certificates to be issued.
•A ***certificate policy*** stating the PKI's requirements concerning its procedures. Its purpose is to allow outsiders to analyze the PKI's trustworthiness.


CA
VA
RA
OK
OK
shop.com

Esoteric protocols

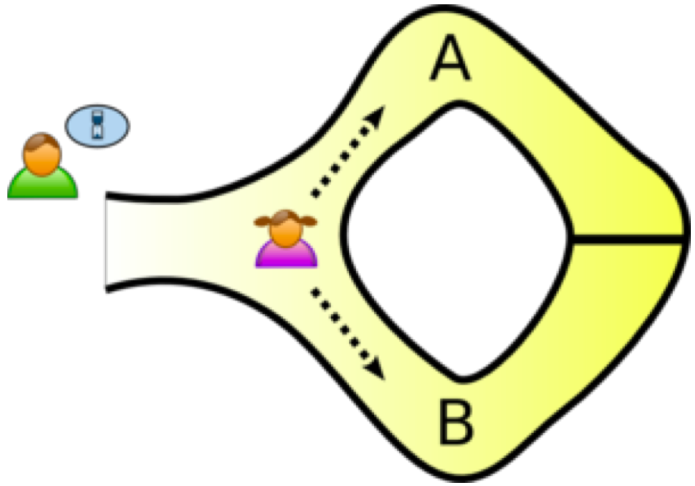
Zero-knowledge proofs

Zero-knowledge proof is a method by which one party (the *prover*) can prove to another party (the *verifier*) that a given statement is true, without conveying any information apart from the fact that the statement is indeed true.

Zero-knowledge proofs

- A zero-knowledge proof must satisfy three properties:
- **Completeness**: if the statement is true, the honest verifier (that is, one following the protocol properly) will be convinced of this fact by an honest prover.
- **Soundness**: if the statement is false, no cheating prover can convince the honest verifier that it is true, except with some small probability.
- **Zero-knowledge**: if the statement is true, no cheating verifier learns anything other than the fact that the statement is true.

The Ali Baba cave



Hamiltonian cycle for a large graph (Manuel Blum)

- At the beginning of each round, Peggy creates *H*, a graph which is isomorphic to *G* (i.e. *H* is just like *G* except that all the vertices have different names). Since it is trivial to translate a Hamiltonian cycle between isomorphic graphs with known isomorphism, if Peggy knows a Hamiltonian cycle for *G* she also must know one for *H*.
- Peggy commits to *H*.
- Victor then randomly chooses one of two questions to ask Peggy. He can either ask her to show the isomorphism between *H* and *G*, or he can ask her to show a Hamiltonian cycle in *H*.
- If Peggy is asked to show that the two graphs are isomorphic, she first uncovers all of *H* (e.g. by turning all pieces of papers that she put on the table).
- If Peggy is asked to prove that she knows a Hamiltonian cycle in *H*, she translates her Hamiltonian cycle in *G* onto *H* and only uncovers the edges on the Hamiltonian cycle.

Blind RSA signatures

- Bob public key: (e, n)
- Alice wants Bob to sign m
- Masking:
  $t = m\, k^e \bmod n$
- Bob signs t
  $t^d = (m\, k^e)^d \bmod n = m^d\, k^{ed} \bmod n$
- Alice deletes the mask
  $s = t^d / k = m^d \bmod n$

Coin flipping

- Alice chooses $1 < x < p$
- Alice calculates $y = g^x \bmod p$
- Alice sends y to Bob
- Bob chooses a bit b and a random k
- Bob calculates $r = y^b g^k \bmod p$ and sends r to Alice
- Alice sends a random bit c to Bob
- Bob sends b and k
- Alice checks $r = y^b g^k \bmod p$

Seminar

Problem 1

For point A=(9;1) in group of points in elliptic curve $y^2 = x^3 - 2x - 8$ over GF(13) compute B=2A=A+A and C=3A=A+A+A

Problem 2

Find the group of points of elliptic curve $y^2 = x^3 - 2x - 5$ over GF(13)
For point A=(3;4) determine is it generator of whole group or only subgroup and show all corresponding points.

Problem 3

Compute the digital signature of message m=5 in GOST R 34.10-2012 We consider the whole group of points of elliptic curve $y^2 = x^3 - 10x - 6$ over GF(13) and point G=(12;4) as a generator. Random parameter for generating digital signature is k=2 and senders open key is Q=(10;7).

Problem 4

Alice and Bob take part in Blom's scheme over modulo p=11. Alice has identification (7,2) and corresponding secret key (3,2), Bob has identification (5,4) and corresponding secret key (1,8). Find their common secret seance key and corresponding secret matrices of trusted authority

Thank you for your attention!!!