Diffie – Hellman

Cryptography and Protocols

Andrei Bulatov

Key Exchange

- Using public key cryptography is expensive.
- A better way is to use it in limited amount to generate a key for a private key cryptosystem
- If p is prime then there is a primitive root modulo p, that is a number g such that $\{1,2,\dots,p-1\}=\{g,g^2,g^3,\dots,g^{p-1}\}$

Key Exchange (cntd)

- Diffie – Hellman protocol:

  - Alice chooses a prime q and finds a primitive root g

  - Alice chooses a random X from $\{1,2,\ldots,q-2\}$ and sends g,q and $\hat{X} \equiv g^X (\mathrm{mod}\ q)$ to Bob

  - Bob chooses random Y from $\{1,2,\ldots,q-2\}$ and sends $\hat{Y} \equiv g^Y (\mathrm{mod}\ q)$ to Alice

  - Alice and Bob compute $k \equiv g^{XY} (mod\ q)$ (by computing $\hat{Y}^X$ and $\hat{X}^Y$ respectively. They use k as a private key

Diffie – Hellman Protocol

$$\text{Alice} \quad \underset{g^{Y}}{\overset{g^{X}}{\rightleftarrows}} \quad \text{Bob}$$

$X \in \mathbb{Z}_p^*$ $\qquad\qquad$ $Y \in \mathbb{Z}_p^*$

$k = \left(g^{Y}\right)^{X}$ $\qquad\qquad$ $k = \left(g^{X}\right)^{Y}$

Diffie – Hellman Protocol

- If Eve can compute discrete logarithm, that is find X and Y, then the protocol is insecure.

  However, this is not enough

- Decisional Diffie – Hellman (DDH) Assumption.

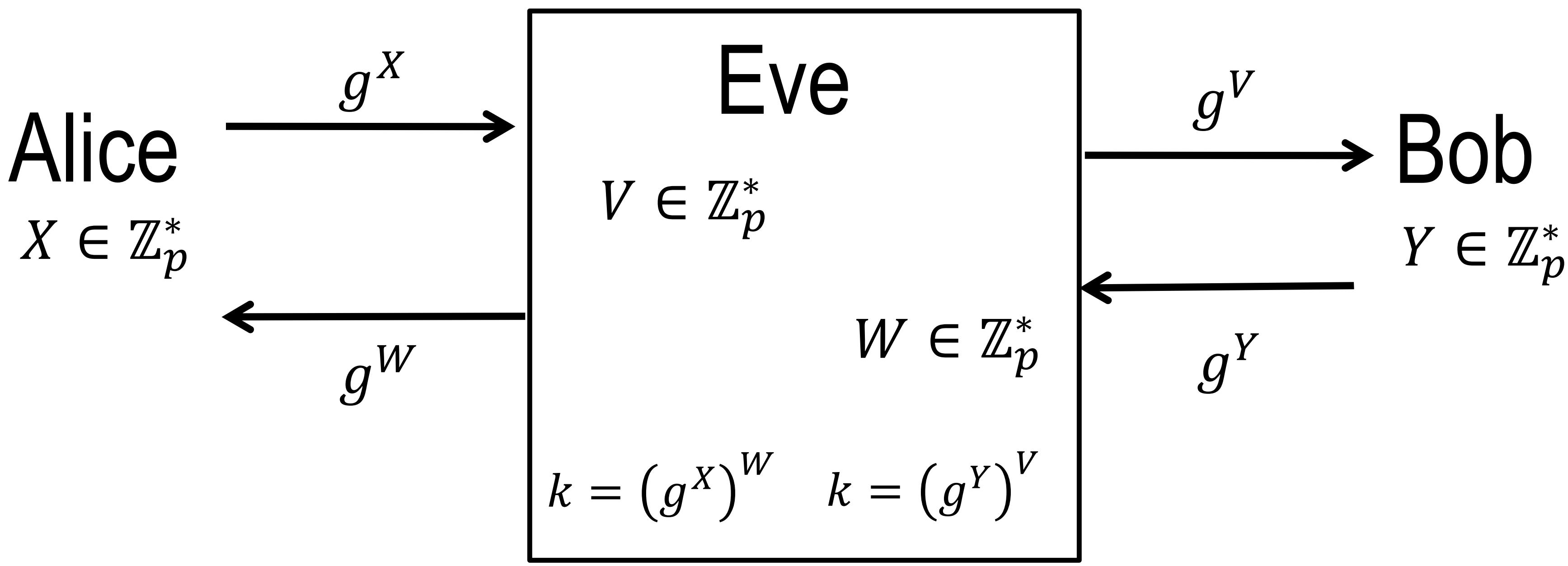
  For every prime p and a primitive root g modulo p the following two distributions over triplets are computationally indistinguishable:

  $\langle g^X, g^Y, g^{XY} \rangle$ — X, Y are random

  $\langle g^X, g^Y, g^Z \rangle$ — X, Y, Z are random

- it is not true !!

Man in the Middle



- Eve masquerades as Bob for Alice and as Alice for Bob.
- So she can read all messages they send

Other Problems

- How do we know that p is prime and g is a primitive root?
- What if Eve replaces g^X with 1?
- What if Eve replaces g^X with an element of small order
- Safe primes:

  $$p = 2q + 1$$

  where q is a prime.

Hard Problems in Number Theory

- **Factorization**:

There is a superpolynomial pair (T,ε) such that for any probabilistic algorithm Alg with time complexity less than $T(n)$ the following holds

Pr[Alg finds factorization of a random n-bit integer] < $\varepsilon(n)$

- **Discrete Logarithm**

There is a superpolynomial pair (T,ε) such that for any probabilistic algorithm Alg with time complexity less than $T(n)$ the following holds:

Pr[given g^X and g, a random primitive root mod p and random X Alg finds X] < $\varepsilon(\log p)$

Factorization

- There are many algorithms for factorization
  - Baby-step giant-step
  - Function field sieve
  - Index calculus algorithm
  - Number field sieve
  - Pohlig–Hellman algorithm
  - Pollard's rho algorithm for logarithms
- Significant success, still cannot factorize long numbers
- RSA challenge
- Smallest number resisting factoring:

RSA-230 = 796949159794106673291612844957324615636756180801260007088891883
553172646341490933493372247868650755230855864199929221814436684722874
052065257937495694348389263171152522525654410980819170611742509702440718010364831638288518852689

El Gamal Encryption Scheme

- K, key generation:

  Choose a prime p and a primitive root g mod p

  Choose random $X \in \mathbb{Z}_p^*$.

  Compute $h = g^X$
- Public key: p, g, h
- Private key: X
- E, encryption:

  Choose random $Y \in \mathbb{Z}_p^*$

  Compute $c_1 = g^Y$ and a shared secret $s = h^Y = g^{XY}$

  Compute $c_2 = P \cdot s$

  Cyphertext $(c_1, c_2) = (g^Y, P \cdot g^{XY})$

El Gamal Encryption Scheme (cntd)

- D, decryption:

  Compute the shared secret $s = c_1^X = \left(g^Y\right)^X = g^{XY}$

  Compute $P = c_2 \cdot s^{-1} = (P \cdot s) \cdot s^{-1}$

Generalizations of El Gamal

- $\mathbb{Z}_p^*$ is a cyclic group – it is generated by the primitive root
- Replace it with some other `efficient' cyclic group
- Examples:

  elliptic curve group

  braid group

  Suzuki 2-group

  Thompson's group

  Baumslag–Solitar group

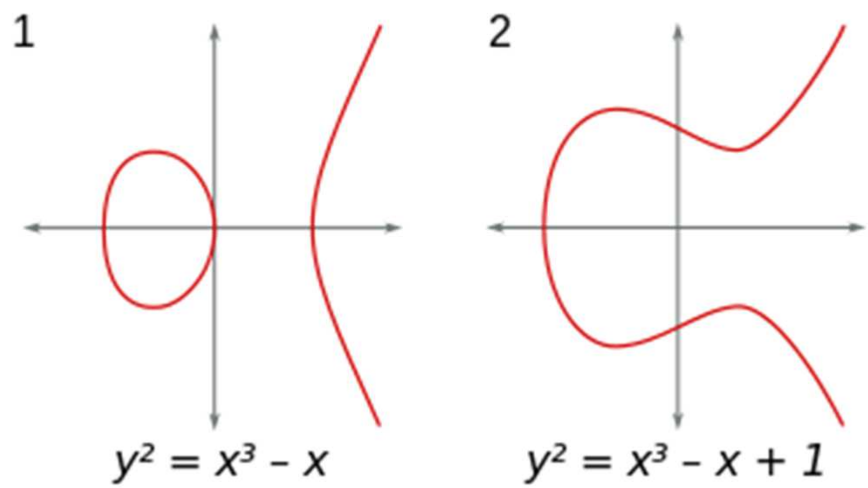
  ....

Elliptic Curves Cryptosystem

- Elliptic curves are defined in algebraic geometry – difficult
- One specific type of elliptic curves

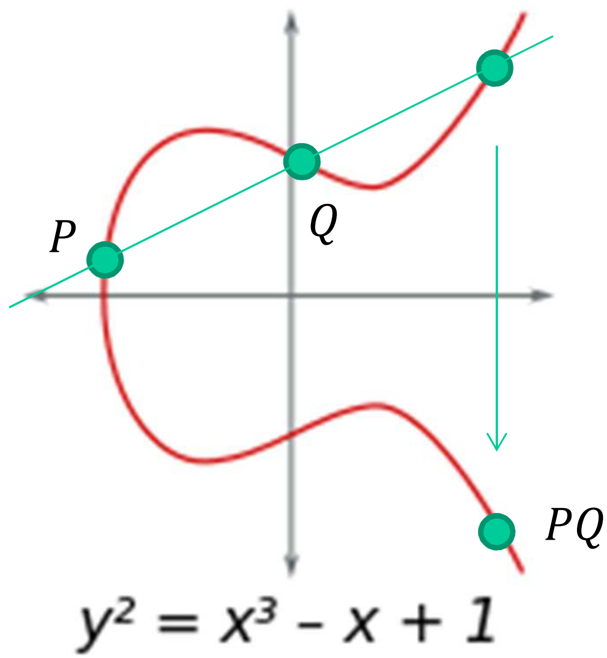
$$y^2 = x^3 + ax + b$$

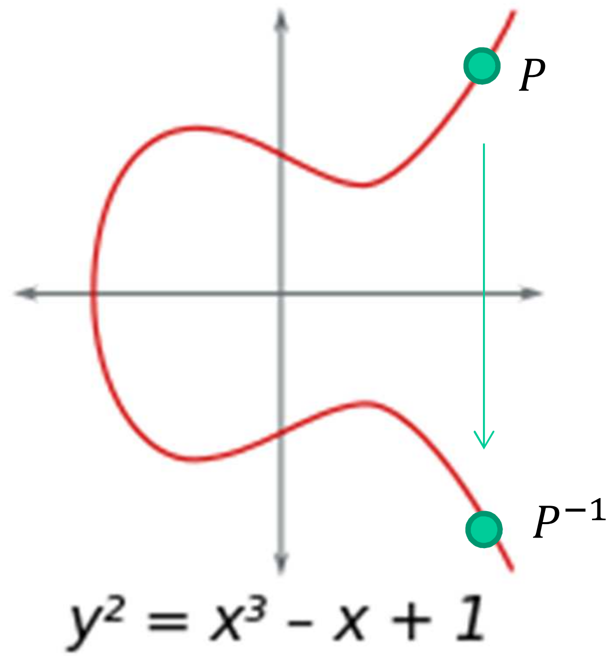
- Depending on the parameters a, b these elliptic curves come in different shapes



Elliptic Curves Group

- We can define group operations on elliptic curves





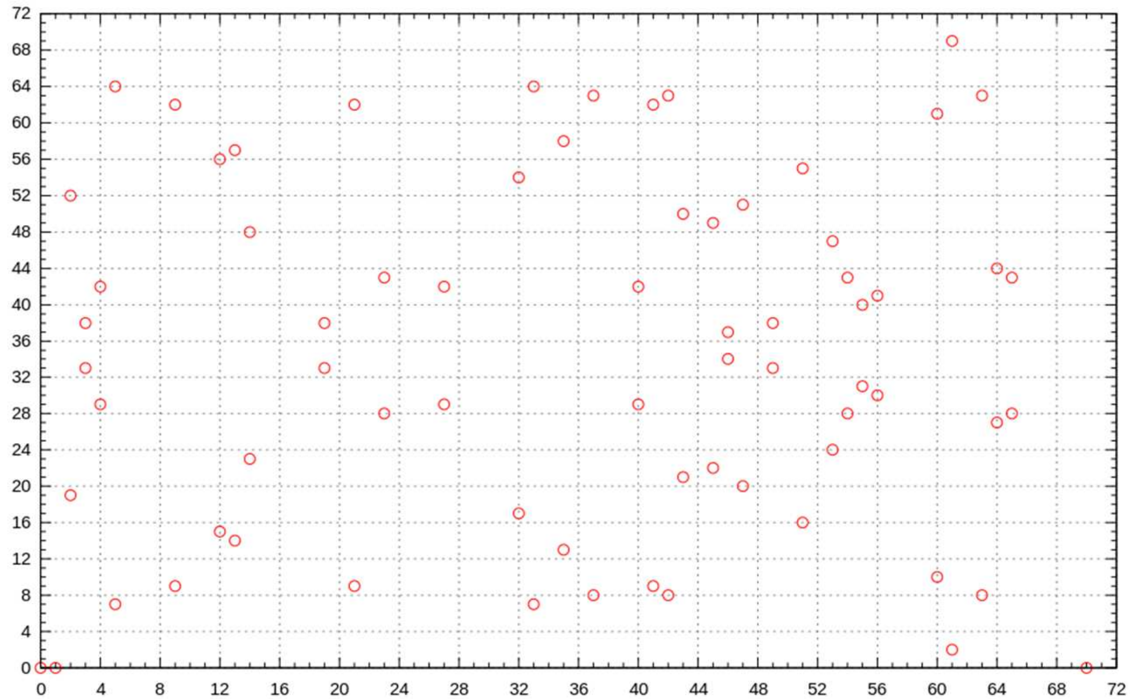
- The unity 1 is the infinite point

Discrete Elliptic Curves Group

- Elliptic curves can be defined over $\mathbb{Z}_p$:
- All pairs (x, y) with $x, y \in \mathbb{Z}_p$ satisfying the equation

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

- This group $E(\mathbb{Z}_p)$ contains approximately p elements



$$y^2 = x^3 - x$$
$$p = 71$$

- Multiplication and inverse can be defined in a \`similar' way