Reviews on PKC
DH
ElGamal
Massey – Omura
Discrete Logarithms
DL Attacks
BSGS
Pohlih–Hellmann
DL records
Square roots
Reminder from Yesterday
Points of finite order
Important Results
Hasse's Theorem
Waterhouse's Theorem
Rück's Theorem
Legendre Symbols
Further reading

ELLIPTIC CURVES CRYPTOGRAPHY

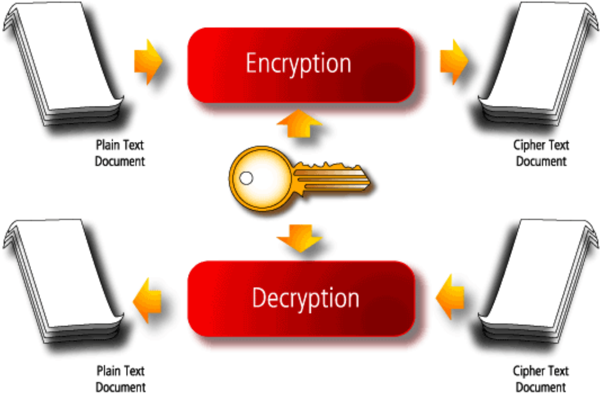
FRANCESCO PAPPALARDI

#2 - SECOND LECTURE.

SEPTEMBER 15TH 2015

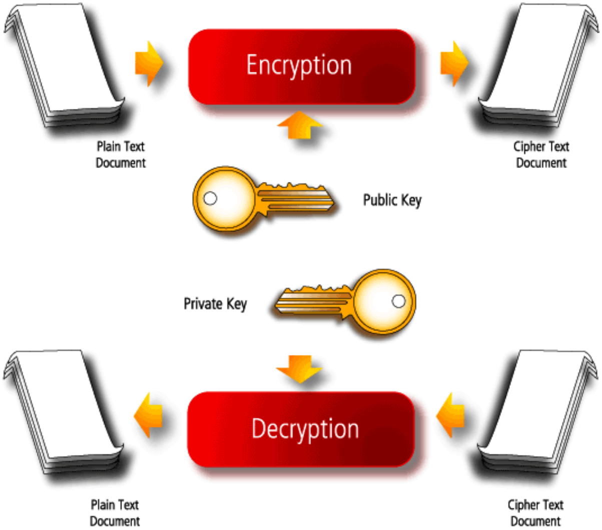
National University of Mongolia
Ulan Baatar, Mongolia
September 15, 2015

Private key versus Public Key



Reviews on PKC
DH
ElGamal
Massey – Omura
Discrete Logarithms
DL Attacks
BSGS
Pohlih–Hellmann
DL records
Square roots
Reminder from Yesterday
Points of finite order
Important Results
Hasse's Theorem
Waterhouse's Theorem
Rück's Theorem
Legendre Symbols
Further reading

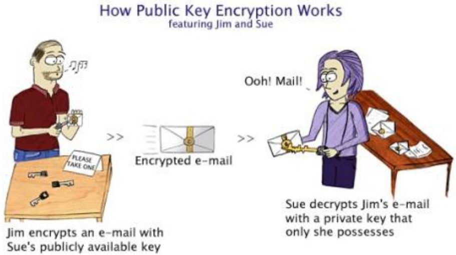
Private key versus Public Key



Reviews on PKC
DH
ElGamal
Massey – Omura
Discrete Logarithms
DL Attacks
BSGS
Pohlih–Hellmann
DL records
Square roots
Reminder from Yesterday
Points of finite order
Important Results
Hasse's Theorem
Waterhouse's Theorem
Rück's Theorem
Legendre Symbols
Further reading

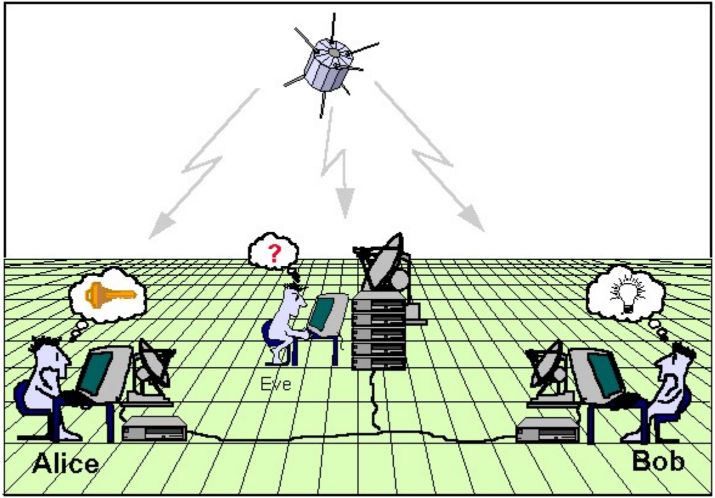
Classical General Examples of PKC

1. (1976) Diffie Hellmann Key exchange protocol *IEEE Trans. Information Theory IT-22 (1976)*
2. (1983) Massey Omura Cryptosystem *Proc. 4^{th} Benelux Symposium on Information Theory (1983)*
3. (1984) ElGamal Cryptosystem *IEEE Trans. Information Theory IT-31 (1985)*



Reviews on PKC
DH
ElGamal
Massey – Omura
Discrete Logarithms
DL Attacks
BSGS
Pohlih–Hellmann
DL records
Square roots
Reminder from Yesterday
Points of finite order
Important Results
Hasse's Theorem
Waterhouse's Theorem
Rück's Theorem
Legendre Symbols
Further reading

PKS



Elliptic curves over $\mathbb{F}_q$

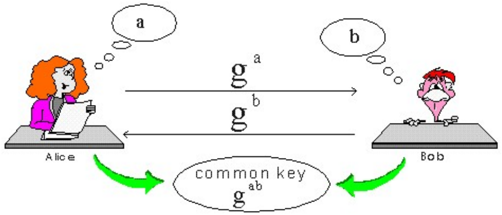
Reviews on PKC
DH
ElGamal
Massey – Omura
Discrete Logarithms
DL Attacks
BSGS
Pohlih–Hellmann
DL records
Square roots
Reminder from Yesterday
Points of finite order
Important Results
Hasse's Theorem
Waterhouse's Theorem
Rück's Theorem
Legendre Symbols
Further reading

Diffie–Hellmann key exchange

Reviews on PKC
DH
ElGamal
Massey – Omura
Discrete Logarithms
DL Attacks
BSGS
Pohlih–Hellmann
DL records
Square roots
Reminder from Yesterday
Points of finite order
Important Results
Hasse's Theorem
Waterhouse's Theorem
Rück's Theorem
Legendre Symbols
Further reading

DHKEP

1. **Alice** and **Bob** agree on a cyclic group G and on a *generator* g in G
2. **Alice** picks a secret a, $0 \leq a \leq |G|$
3. **Bob** picks a secret b, $0 \leq b \leq |G|$
4. They compute and publish g^a (**Alice**) and g^b (**Bob**)
5. The common secret key is g^{ab}



Reviews on PKC
DH
ElGamal
Massey – Omura
Discrete Logarithms
DL Attacks
BSGS
Pohlih–Hellmann
DL records
Square roots
Reminder from Yesterday
Points of finite order
Important Results
Hasse's Theorem
Waterhouse's Theorem
Rück's Theorem
Legendre Symbols
Further reading

ElGamal Cryptosystem

Alice wants to sent a message $x \in G$ (cyclic group) to **Bob**

ElGamal SETUP:

1. **Alice** and **Bob** agree on a *generator* g in G
2. **Bob** picks a secret b, $0 < b \leq |G|$, he computes $\beta = g^b \in G$ and publishes β

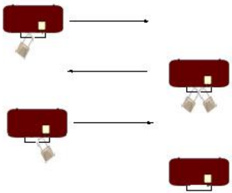
ElGamal ENCRYPTION: (Alice)

1. **Alice** picks a secret k, $0 < k \leq |G|$
2. She computes $\alpha = g^k \in G$ and $\gamma = x \cdot \beta^k \in G$
3. The encrypted message is $E(x) = (\alpha, \gamma) \in G \times G$

ElGamal DECRYPTION: (Bob)

1. **Bob** computes $D(\alpha, \gamma) = \gamma \cdot \alpha^{|G|-b}$
2. It works since $D(E(x)) = D(\alpha, \gamma) = x \cdot g^{bk} \cdot g^{k(|G|-b)} = x$ since $g^{k|G|} = 1$

Massey Omura on any finite Group G



Alice **Bob**

SETUP:

① **Alice** and **Bob** each
- pick a secret key $k_A, k_B \in U(\mathbb{Z}/|G|\mathbb{Z})$
- compute $\ell_A, \ell_B \in U(\mathbb{Z}/|G|\mathbb{Z})$ such that $k_A\ell_A \equiv 1(\mathrm{mod}\,|G|)$ and $k_B\ell_B \equiv 1(\mathrm{mod}\,|G|)$

④ **Alice** key is (k_A, ℓ_A) (k_A to lock and ℓ_A to unlock)

⑤ **Bob** key is (k_B, ℓ_B) (k_B to lock and ℓ_B to unlock)

WORKING: To send the message P

① **Alice** computes and sends $M = P^{k_A} \in G$

② **Bob** computes and sends back $N = M^{k_B} \in G$

③ **Alice** computes $L = N^{\ell_A} \in G$ and sends it back to **Bob**

④ **Bob** decrypt the message computing $P = L^{\ell_B} \in G$

It works: $P = L^{\ell_B} = N^{\ell_A \ell_B} = M^{k_B \ell_A l_B} = P^{k_A k_B \ell_A \ell_B} \in G$

Reviews on PKC
DH
ElGamal
Massey – Omura
Discrete Logarithms
DL Attacks
BSGS
Pohlih–Hellmann
DL records
Square roots
Reminder from Yesterday
Points of finite order
Important Results
Hasse's Theorem
Waterhouse's Theorem
Rück's Theorem
Legendre Symbols
Further reading

The generic Discrete Logarithms problem

- $G = \langle g \rangle$ cyclic group
- g a generator
- $x \in G$

Discrete Logarithm Problem:

Find $n \in \mathbb{Z}/|G|\mathbb{Z}$ such that $x = g^n$

- Need to specify how to make the operations in G
- If $G = (\mathbb{Z}/n\mathbb{Z}, +)$ then discrete logs are very easy.
- If $G = ((\mathbb{Z}/n\mathbb{Z})^*, \times)$ then G is cyclic iff $n = 2, 4, p^\alpha, 2 \cdot p^\alpha$ where p is an odd prime: famous theorem of Gauß.
- In $G = (\mathbb{Z}/p\mathbb{Z})^* =: \mathbb{F}_p^*$ there is no efficient algorithm to compute DL.
- We are interested in the case when $G = E(\mathbb{F}_q)$ where $E/\mathbb{F}_q$ is an elliptic curve
- Primordial public key cryptography is based on the difficulty of the Discrete Log problem

Reviews on PKC
DH
ElGamal
Massey – Omura
Discrete Logarithms
DL Attacks
BSGS
Pohlih–Hellmann
DL records
Square roots
Reminder from Yesterday
Points of finite order
Important Results
Hasse's Theorem
Waterhouse's Theorem
Rück's Theorem
Legendre Symbols
Further reading

Classical DL attacks

- Shanks baby-step, giant step (BSGS) *Proc. 2^{nd} Manitoba Conf. Numerical Mathematics (Winnipeg, 1972).*
- Pohlig–Hellmann Algorithm *IEEE Trans. Information Theory IT-24 (1978).*
- Index computation algorithm
- Sieving algorithms *La Macchia & Odlyzko, Designs Codes and Cryptography 1 (1991)*

NOTE: The last two are "very special" for $\mathbb{F}_q^*$

Elliptic curves over $\mathbb{F}_q$
Reviews on PKC
DH
ElGamal
Massey – Omura
Discrete Logarithms
DL Attacks
BSGS
Pohlih–Hellmann
DL records
Square roots
Reminder from Yesterday
Points of finite order
Important Results
Hasse's Theorem
Waterhouse's Theorem
Rück's Theorem
Legendre Symbols
Further reading

DISCRETE LOGARITHMS: continues

Shanks Baby Step Giant Step algorithm

```
Input:   A group G = ⟨g⟩ and a ∈ G
Output:   k ∈ ℤ/|G|ℤ such that a = g^k
1.   M := ⌈√|G|⌉
2.   For j = 0,1,2,...,M.
           Compute g^j and store the pair (j, g^j) in a table
3.   A := g^{-M},  B := a
5.   For i = 0,1,2,...,M − 1.
         -1- Check if B is the second component (g^j) of any
              pair in the table
         -2- If so, return iM + j and halt.
         -3- If not B = B · A
```

- The BSGS algorithm is a generic algorithm. It works for every finite cyclic group.
- based on the fact that $\forall x \in \mathbb{Z}/n\mathbb{Z}$, $x = j + im$ with $m = \lceil\sqrt{n}\rceil$, $0 \le j < m$ and $0 \le i < m$
- Not necessary to know the order of the group G in advance. The algorithm still works if an upper bound on the group order is known.
- Usually the BSGS algorithm is used for groups whose order is prime.
- The running time of the algorithm and the space complexity is $O(\sqrt{|G|})$, much better than the $O(|G|)$ running time of the naive brute force
- The algorithm was originally developed by Daniel Shanks.

Reviews on PKC
DH
ElGamal
Massey – Omura
Discrete Logarithms
DL Attacks
BSGS
Pohlih–Hellmann
DL records
Square roots
Reminder from Yesterday
Points of finite order
Important Results
Hasse's Theorem
Waterhouse's Theorem
Rück's Theorem
Legendre Symbols
Further reading

DISCRETE LOGARITHMS: continues

The Pohlig–Hellman Algorithm

In some groups Discrete logs are easy. For example if G is a cyclic group and $\#G = 2^m$ then we know that there are subgroups:

$$\langle 1 \rangle = G_0 \subset G_1 \subset \cdots \subset G_m = G$$

such that G_i is cyclic and $\#G_i = 2^i$. Furthermore

$$G_i = \left\{ y \in G \text{ such that } y^{2^i} = 1 \right\}.$$

If $G = \langle g \rangle$, for any $a \in G$, either $a^{2^{m-1}} = 1$ or $a^{2^{m-1}} = g^{2^{m-1}}$. From this property we deduce the algorithm:

```
Input:   A group G = ⟨g⟩, |G| = 2^m and a ∈ G
Output:  k ∈ Z/|G|Z such that a = g^k
1.  A := a,  K = 0
2.  For j = 1,2,...,m.
          If A^(2^(m-j)) ≠ 1,  A := g^(-2^(j-1)) · A; K := K + 2^(j-1)
3.  Output K
```

Reviews on PKC
DH
ElGamal
Massey – Omura
Discrete Logarithms
DL Attacks
BSGS
Pohlih–Hellmann
DL records
Square roots
Reminder from Yesterday
Points of finite order
Important Results
Hasse's Theorem
Waterhouse's Theorem
Rück's Theorem
Legendre Symbols
Further reading

DISCRETE LOGARITHMS: continues

The Pohlig–Hellman Algorithm

- The above is a special case of the Pohlig-Hellman Algorithm which can be extended to the case when $|G|$ has only small prime divisors
- To avoid this situation one crucial requirement for a DL-resistent group in cryptography is that $\#G$ has a large prime divisor
- If $p = 2^k + 1$ is a Fermat prime, then DL in $(\mathbb{F}_p)^*$ are easy
- Classical algorithm for factoring have often analogues for computing discrete logs. A very important one is the *Pollard ρ–method*
- One of the strongest algorithms is the index calculus algorithm. NOT generic. It works only in $\mathbb{F}_q^*$

Reviews on PKC
DH
ElGamal
Massey – Omura
Discrete Logarithms
DL Attacks
BSGS
Pohlih–Hellmann
DL records
Square roots
Reminder from Yesterday
Points of finite order
Important Results
Hasse's Theorem
Waterhouse's Theorem
Rück's Theorem
Legendre Symbols
Further reading

DISCRETE LOGARITHMS: continues

Records

Discrete Logarithm Records:

- $G = \mathbb{F}_p^*$: $p \approx 10^{180}$ (596-bit)
  Cyril Bouvier, Pierrick Gaudry, Laurent Imbert, Hamza Jeljeli and Emmanuel Thomé (11 June 2014)
- $G = \mathbb{F}_{p^2}^*$: $p \approx 10^{80}$
  Razvan Barbulescu, Pierrick Gaudry, Aurore Guillevic, and François Morain (25 June 2014)
- $G = \mathbb{F}_{2^\alpha}^*$: $\alpha = 1279$
  Thorsten Kleinjung (17 October 2014)
- $G = E(\mathbb{F}_p)$: $p \approx 10^{35}$
  Joppe W. Bos, Marcelo E. Kaihara, T. Kleinjung, Arjen K. Lenstra and Peter L. Montgomery (July 2009)
  $p = 4451685225093714772084598273548427$
- $G = E(\mathbb{F}_{2^\alpha})$: $\alpha = 113$ Erich Wenger and Paul Wolfger (January 2015)

with *ECC* same security with $1/5$ of the size

Reviews on PKC
DH
ElGamal
Massey – Omura
Discrete Logarithms
DL Attacks
BSGS
Pohlih–Hellmann
DL records
Square roots
Reminder from Yesterday
Points of finite order
Important Results
Hasse's Theorem
Waterhouse's Theorem
Rück's Theorem
Legendre Symbols
Further reading

The problem of "Square Roots Modulo a prime"

Given an odd prime p and a quadratic residue a

Find x such that $x^2 \equiv a \bmod p$

It can be solved efficiently if we are given a quadratic nonresidue $g \in (\mathbb{Z}/p\mathbb{Z})^*$

1. Write $p-1 = 2^k \cdot q$ and we know that $(\mathbb{Z}/p\mathbb{Z})^*$ has a (cyclic) subgroup G with 2^k elements.
2. Note that $b = g^q$ is a generator of G (in fact if it was $b^{2^j} \equiv 1 \bmod p$ for $j < k$, then $g^{(p-1)/2} \equiv 1 \bmod p$) and that $a^q \in G$
3. Use the last algorithm to compute t such that $a^q = b^t$. Note that t is even since $a^{(p-1)/2} \equiv 1 \bmod p$.
4. Finally set $x = a^{(p-q)/2} b^{t/2}$ and observe that $x^2 = a^{(p-q)} b^t = a^p \equiv a \bmod p$.

REMARKS:

- The above is not deterministic. However Schoof in 1985 discovered a polynomial time algorithm which is however not efficient.
- To find a random point in an elliptic curve $E/\mathbb{F}_p$ one needs to compute square roots modulo p

Reviews on PKC
DH
ElGamal
Massey – Omura
Discrete Logarithms
DL Attacks
BSGS
Pohlih–Hellmann
DL records
Square roots
Reminder from Yesterday
Points of finite order
Important Results
Hasse's Theorem
Waterhouse's Theorem
Rück's Theorem
Legendre Symbols
Further reading

The problem of "Modular Square Roots"

Reviews on PKC
DH
ElGamal
Massey – Omura
Discrete Logarithms
DL Attacks
BSGS
Pohlih–Hellmann
DL records
Square roots
Reminder from Yesterday
Points of finite order
Important Results
Hasse's Theorem
Waterhouse's Theorem
Rück's Theorem
Legendre Symbols
Further reading

Given $n, a \in \mathbb{N}$

Find x (if it exists) such that $x^2 \equiv a \bmod n$

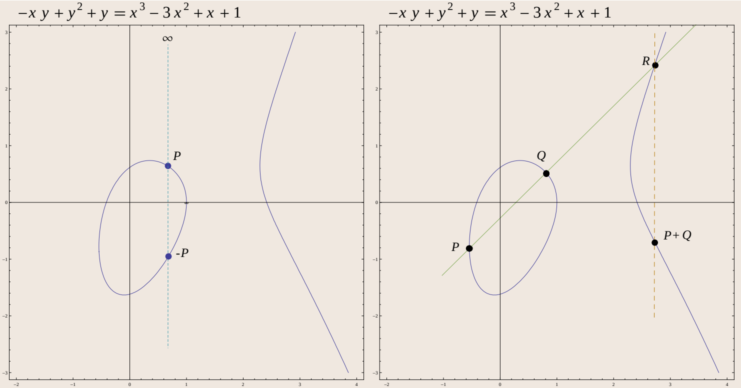
If the factorization of n is known, then this problem (efficiently) can be solved in 3 steps:

1. For each prime divisor p of n find x_p such that $x_p^2 \equiv a \bmod p$
2. Use the Hensel's Lemma to lift x_p to y_p where $y_p^2 \equiv a \bmod p^{v_p(n)}$
3. Use the Chinese remainder Theorem to find $x \in \mathbb{Z}/n\mathbb{Z}$ such that $x \equiv y_p \bmod p^{v_p(n)} \; \forall p \mid n$.
4. Finally $x^2 \equiv a \bmod n$.

Reminder from Yesterday

If $P, Q \in E(\mathbb{F}_q)$, $r_{P,Q}$: $\begin{cases} \text{line through } P \text{ and } Q & \text{if } P \neq Q \\ \text{tangent line to } E \text{ at } P & \text{if } P = Q, \end{cases}$

$r_{P,\infty}$: vertical line through P



$r_{P,\infty} \cap E(\mathbb{F}_q) = \{P, \infty, P'\}$ $\rightsquigarrow$ $\boxed{-P := P'}$

$r_{P,Q} \cap E(\mathbb{F}_q) = \{P, Q, R\}$ $\rightsquigarrow$ $\boxed{P +_E Q := -R}$

Formulas for Addition on E (Summary)

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

$P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(\mathbb{F}_q) \setminus \{\infty\}$,

Addition Laws for the sum of affine points

- If $P_1 \neq P_2$
  - $x_1 = x_2$ $\Rightarrow$ $P_1 +_E P_2 = \infty$
  - $x_1 \neq x_2$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$$

- If $P_1 = P_2$
  - $2y_1 + a_1 x + a_3 = 0$ $\Rightarrow$ $P_1 +_E P_2 = 2P_1 = \infty$
  - $2y_1 + a_1 x + a_3 \neq 0$

$$\lambda = \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x + a_3}, \nu = -\frac{a_3 y_1 + x_1^3 - a_4 x_1 - 2a_6}{2y_1 + a_1 x_1 + a_3}$$

Then

$$P_1 +_E P_2 = (\lambda^2 - a_1 \lambda - a_2 - x_1 - x_2, -\lambda^3 - a_1^2 \lambda + (\lambda + a_1)(a_2 + x_1 + x_2) - a_3 - \nu)$$

Formulas for Addition on E (Summary for special equation)

$$E : y^2 = x^3 + Ax + B$$

$P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(\mathbb{F}_q) \setminus \{\infty\}$,

Addition Laws for the sum of affine points

- If $P_1 \neq P_2$
  - $x_1 = x_2$ $\Rightarrow$ $P_1 +_E P_2 = \infty$
  - $x_1 \neq x_2$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$$

- If $P_1 = P_2$
  - $y_1 = 0$ $\Rightarrow$ $P_1 +_E P_2 = 2P_1 = \infty$
  - $y_1 \neq 0$

$$\lambda = \frac{3x_1^2 + A}{2y_1}, \nu = -\frac{x_1^3 - Ax_1 - 2B}{2y_1}$$

Then

$$P_1 +_E P_2 = (\lambda^2 - x_1 - x_2, -\lambda^3 + \lambda(x_1 + x_2) - \nu)$$

Reviews on PKC
DH
ElGamal
Massey – Omura
Discrete Logarithms
DL Attacks
BSGS
Pohlih–Hellmann
DL records
Square roots
Reminder from Yesterday
Points of finite order
Important Results
Hasse's Theorem
Waterhouse's Theorem
Rück's Theorem
Legendre Symbols
Further reading

The division polynomials

Definition (Division Polynomials of $E : y^2 = x^3 + Ax + B$ ($p > 3$))

$$
\begin{aligned}
\psi_0 &= 0,\ \psi_1 = 1,\ \psi_2 = 2y \\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\
&\vdots \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \qquad \text{for } m \geq 2 \\
\psi_{2m} &= \left(\frac{\psi_m}{2y}\right) \cdot (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \quad \text{for } m \geq 3
\end{aligned}
$$

The polynomial $\psi_m \in \mathbb{Z}[x, y]$ is the m^{th} *division polynomial*

Theorem ($E : Y^2 = X^3 + AX + B$ elliptic curve, $P = (x, y) \in E$)

$$mP = m(x, y) = \left(\frac{\phi_m(x)}{\psi_m^2(x)}, \frac{\omega_m(x, y)}{\psi_m^3(x, y)}\right),$$

where $\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}$, $\omega_m = \dfrac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{4y}$

Points of order m

Definition (m–torsion point)

Let E/K and let $\bar{K}$ an *algebraic closure of* K.

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

Theorem (Structure of Torsion Points)

Let E/K and $m \in \mathbb{N}$.

$$E[m] \cong \begin{cases} C_m \oplus C_m & \text{if } p = \mathrm{char}(K) \nmid m \\ C_m \oplus C_{m'} \quad \text{or} \quad E[m] \cong C_{m'} \oplus C_{m'} & \text{if } m = p^r m', p \nmid m' \end{cases}$$

FACTS:

- $E[2m+1] \setminus \{\infty\} = \{(x,y) \in E(\bar{K}) : \ \psi_{2m+1}(x) = 0\}$
- $E[2m] \setminus E[2] = \{(x,y) \in E(\bar{K}) : \ y^{-1}\psi_{2m}(x) = 0\}$
- Corollary of the Theorem of Structure for torsion $\exists n, k \in \mathbb{N}$ such that $E(\mathbb{F}_q) \cong C_n \oplus C_{nk}$
- Property of Weil pairing $n \mid q-1$.

Reviews on PKC
DH
ElGamal
Massey – Omura
Discrete Logarithms
DL Attacks
BSGS
Pohlih–Hellmann
DL records
Square roots
Reminder from Yesterday
Points of finite order
Important Results
Hasse's Theorem
Waterhouse's Theorem
Rück's Theorem
Legendre Symbols
Further reading

Theorem (Hasse)

Let E be an elliptic curve over the finite field $\mathbb{F}_q$. Then the order of $E(\mathbb{F}_q)$ satisfies

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

So $\#E(\mathbb{F}_q) \in [(\sqrt{q}-1)^2, (\sqrt{q}+1)^2]$ the *Hasse interval* $\mathcal{I}_q$

Example (Hasse Intervals)

q	$\mathcal{I}_q$
2	$\{1,2,3,4,5\}$
3	$\{1,2,3,4,5,6,7\}$
4	$\{1,2,3,4,5,6,7,8,9\}$
5	$\{2,3,4,5,6,7,8,9,10\}$
7	$\{3,4,5,6,7,8,9,10,11,12,13\}$
8	$\{4,5,6,7,8,9,10,11,12,13,14\}$
9	$\{4,5,6,7,8,9,10,11,12,13,14,15,16\}$
11	$\{6,7,8,9,10,11,12,13,14,15,16,17,18\}$
13	$\{7,8,9,10,11,12,13,14,15,16,17,18,19,20,21\}$
16	$\{9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,25\}$
17	$\{10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26\}$
19	$\{12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28\}$
23	$\{15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33\}$
25	$\{16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36\}$
27	$\{18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38\}$
29	$\{20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40\}$
31	$\{21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43\}$
32	$\{22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44\}$

Reviews on PKC
DH
ElGamal
Massey – Omura
Discrete Logarithms
DL Attacks
BSGS
Pohlih–Hellmann
DL records
Square roots
Reminder from Yesterday
Points of finite order
Important Results
Hasse's Theorem
Waterhouse's Theorem
Rück's Theorem
Legendre Symbols
Further reading

Reviews on PKC
DH
ElGamal
Massey – Omura
Discrete Logarithms
DL Attacks
BSGS
Pohlih–Hellmann
DL records
Square roots
Reminder from Yesterday
Points of finite order
Important Results
Hasse's Theorem
Waterhouse's Theorem
Rück's Theorem
Legendre Symbols
Further reading

Theorem (Waterhouse)

Let $q = p^n$ and let $N = q + 1 - a$.

$$\exists E/\mathbb{F}_q \text{ s.t.} \#E(\mathbb{F}_q) = N \Leftrightarrow |a| \leq 2\sqrt{q} \text{ and}$$

one of the following is satisfied:

(i) $\gcd(a, p) = 1$;

(ii) *n even and one of the following is satisfied:*
1. $a = \pm 2\sqrt{q}$;
2. $p \not\equiv 1 \pmod 3$, *and* $a = \pm\sqrt{q}$;
3. $p \not\equiv 1 \pmod 4$, *and* $a = 0$;

(iii) *n is odd, and one of the following is satisfied:*
1. $p = 2$ *or* 3, *and* $a = \pm p^{(n+1)/2}$;
2. $a = 0$.

Example (q prime $\forall N \in I_q, \exists E/\mathbb{F}_q, \#E(\mathbb{F}_q) = N$. q not prime:)

q	$a \in$
$4 = 2^2$	$\{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$
$8 = 2^3$	$\{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$
$9 = 3^2$	$\{-6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}$
$16 = 2^4$	$\{-8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8\}$
$25 = 5^2$	$\{-10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$27 = 3^3$	$\{-10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$32 = 2^5$	$\{-11, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

Theorem (Rück)

Suppose N is a possible order of an elliptic curve $/\mathbb{F}_q$, $q = p^n$. Write

$$N = p^e n_1 n_2, \quad p \nmid n_1 n_2 \quad \text{and} \quad n_1 \mid n_2 \text{ (possibly } n_1 = 1).$$

There exists $E/\mathbb{F}_q$ s.t.

$$E(\mathbb{F}_q) \cong C_{n_1} \oplus C_{n_2 p^e}$$

if and only if

1. *$n_1 = n_2$ in the case (ii).1 of Waterhouse's Theorem;*
2. *$n_1 | q - 1$ in all other cases of Waterhouse's Theorem.*

Example

- If $q = p^{2n}$ and $\#E(\mathbb{F}_q) = q + 1 \pm 2\sqrt{q} = (p^n \pm 1)^2$, then
$$E(\mathbb{F}_q) \cong C_{p^n \pm 1} \oplus C_{p^n \pm 1}.$$
- Let $N = 100$ and $q = 101 \Rightarrow \exists E_1, E_2, E_3, E_4/\mathbb{F}_{101}$ s.t.
$$E_1(\mathbb{F}_{101}) \cong C_{10} \oplus C_{10} \qquad E_2(\mathbb{F}_{101}) \cong C_2 \oplus C_{50}$$
$$E_3(\mathbb{F}_{101}) \cong C_5 \oplus C_{20} \qquad E_4(\mathbb{F}_{101}) \cong C_{100}$$

Reviews on PKC
DH
ElGamal
Massey – Omura
Discrete Logarithms
DL Attacks
BSGS
Pohlih–Hellmann
DL records
Square roots
Reminder from Yesterday
Points of finite order
Important Results
Hasse's Theorem
Waterhouse's Theorem
Rück's Theorem
Legendre Symbols
Further reading

Subfield curves

Definition

Let $E/\mathbb{F}_q$ and write $E(\mathbb{F}_q) = q + 1 - a$, ($|a| \leq 2\sqrt{q}$). The *characteristic* polynomial of E is

$$P_E(T) = T^2 - aT + q \in \mathbb{Z}[T].$$

and its roots:

$$\alpha = \frac{1}{2}\left(a + \sqrt{a^2 - 4q}\right) \qquad \beta = \frac{1}{2}\left(a - \sqrt{a^2 - 4q}\right)$$

are called *characteristic roots of Frobenius* ($P_E(\Phi_q) = 0$).

Theorem

$\forall n \in \mathbb{N}$

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n).$$

Reviews on PKC
DH
ElGamal
Massey – Omura
Discrete Logarithms
DL Attacks
BSGS
Pohlih–Hellmann
DL records
Square roots
Reminder from Yesterday
Points of finite order
Important Results
Hasse's Theorem
Waterhouse's Theorem
Rück's Theorem
Legendre Symbols
Further reading

Subfield curves (continues)

$$E(\mathbb{F}_q) = q + 1 - a \;\Rightarrow\; E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$

where $P_E(T) = T^2 - aT + q = (T - \alpha)(T - \beta) \in \mathbb{Z}[T]$

Curves $/\mathbb{F}_2$

E	a	$P_E(T)$	(α, β)
$y^2 + xy = x^3 + x^2 + 1$	1	$T^2 - T + 2$	$\frac{1}{2}(1 \pm \sqrt{-7})$
$y^2 + xy = x^3 + 1$	-1	$T^2 + T + 2$	$\frac{1}{2}(-1 \pm \sqrt{-7})$
$y^2 + y = x^3 + x$	-2	$T^2 + 2T + 2$	$-1 \pm i$
$y^2 + y = x^3 + x + 1$	2	$T^2 - 2T + 2$	$1 \pm i$
$y^2 + y = x^3$	0	$T^2 + 2$	$\pm\sqrt{-2}$

$$E: y^2 + xy = x^3 + x^2 + 1 \;\Rightarrow\; E(\mathbb{F}_{2^{100}}) = 2^{100} + 1 - \left(\frac{1+\sqrt{-7}}{2}\right)^{100} - \left(\frac{1-\sqrt{-7}}{2}\right)^{100} = 1267650600228229382588845215376$$

Reviews on PKC
DH
ElGamal
Massey – Omura
Discrete Logarithms
DL Attacks
BSGS
Pohlih–Hellmann
DL records
Square roots
Reminder from Yesterday
Points of finite order
Important Results
Hasse's Theorem
Waterhouse's Theorem
Rück's Theorem
Legendre Symbols
Further reading

Subfield curves

$$E(\mathbb{F}_q) = q + 1 - a \ \Rightarrow\ E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$
$$\text{where } P_E(T) = T^2 - aT + q = (T - \alpha)(T - \beta) \in \mathbb{Z}[T]$$

Curves $/\mathbb{F}_3$

i	E_i	a	$P_{E_i}(T)$	(α, β)
1	$y^2 = x^3 + x$	0	$T^2 + 3$	$\pm\sqrt{-3}$
2	$y^2 = x^3 - x$	0	$T^2 + 3$	$\pm\sqrt{-3}$
3	$y^2 = x^3 - x + 1$	-3	$T^2 + 3T + 3$	$\frac{1}{2}(-3 \pm \sqrt{-3})$
4	$y^2 = x^3 - x - 1$	3	$T^2 - 3T + 3$	$\frac{1}{2}(3 \pm \sqrt{-3})$
5	$y^2 = x^3 + x^2 - 1$	1	$T^2 - T + 3$	$\frac{1}{2}(1 \pm \sqrt{-11})$
6	$y^2 = x^3 - x^2 + 1$	-1	$T^2 + T + 3$	$\frac{1}{2}(-1 \pm \sqrt{-11})$
7	$y^2 = x^3 + x^2 + 1$	-2	$T^2 + 2T + 3$	$-1 \pm \sqrt{-2}$
8	$y^2 = x^3 - x^2 - 1$	2	$T^2 - 2T + 3$	$1 \pm \sqrt{-2}$

Lemma

Let $s_n = \alpha^n + \beta^n$ where $\alpha\beta = q$ and $\alpha + \beta = a$. Then

$$s_0 = 2, \quad , s_1 = a \quad \textit{and} \quad s_{n+1} = as_n - qs_{n-1}$$

Reviews on PKC
- DH
- ElGamal
- Massey – Omura

Discrete Logarithms
- DL Attacks
- BSGS
- Pohlih–Hellmann
- DL records

Square roots

Reminder from Yesterday
- Points of finite order

Important Results
- Hasse's Theorem
- Waterhouse's Theorem
- Rück's Theorem

Legendre Symbols

Further reading

Legendre Symbols

Recall the *Finite field Legendre symbols*: let $x \in \mathbb{F}_q$,

$$\left(\frac{x}{\mathbb{F}_q}\right) = \begin{cases} +1 & \text{if } t^2 = x \text{ has a solution } t \in \mathbb{F}_q^* \\ -1 & \text{if } t^2 = x \text{ has no solution } t \in \mathbb{F}_q \\ 0 & \text{if } x = 0 \end{cases}$$

Theorem

Let $E : y^2 = x^3 + Ax + B$ *over* $\mathbb{F}_q$. *Then*

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3+Ax+B}{\mathbb{F}_q}\right)$$

Proof.

Note that

$$1 + \left(\frac{x_0^3+Ax_0+B}{\mathbb{F}_q}\right) = \begin{cases} 2 & \text{if } \exists y_0 \in \mathbb{F}_q^* \text{ s.t. } (x_0, \pm y_0) \in E(\mathbb{F}_q) \\ 1 & \text{if } (x_0, 0) \in E(\mathbb{F}_q) \\ 0 & \text{otherwise} \end{cases}$$

Hence

$$\#E(\mathbb{F}_q) = 1 + \sum_{x \in \mathbb{F}_q} \left(1 + \left(\frac{x^3+Ax+B}{\mathbb{F}_q}\right)\right)$$

□

Last Slide

Corollary

Let $E: y^2 = x^3 + Ax + B$ *over* $\mathbb{F}_q$ *and* $E_\mu: y^2 = x^3 + \mu^2 Ax + \mu^3 B$, $\mu \in \mathbb{F}_q^* \setminus (\mathbb{F}_q^*)^2$ *its twist. Then*

$$\boxed{\#E(\mathbb{F}_q) = q + 1 - a \Leftrightarrow \#E_\mu(\mathbb{F}_q) = q + 1 + a}$$

and

$$\boxed{\#E(\mathbb{F}_{q^2}) = \#E_\mu(\mathbb{F}_{q^2}).}$$

Proof.

$$\begin{aligned}\#E_\mu(\mathbb{F}_q) &= q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + \mu^2 Ax + \mu^3 B}{\mathbb{F}_q}\right) \\ &= q + 1 + \left(\frac{\mu}{\mathbb{F}_q}\right) \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + Ax + B}{\mathbb{F}_q}\right)\end{aligned}$$

and $\left(\frac{\mu}{\mathbb{F}_q}\right) = -1$ □

Reviews on PKC
DH
ElGamal
Massey – Omura
Discrete Logarithms
DL Attacks
BSGS
Pohlih–Hellmann
DL records
Square roots
Reminder from Yesterday
Points of finite order
Important Results
Hasse's Theorem
Waterhouse's Theorem
Rück's Theorem
Legendre Symbols
Further reading

Further Reading...

Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart, Advances in elliptic curve cryptography, London Mathematical Society Lecture Note Series, vol. 317, Cambridge University Press, Cambridge, 2005.

J. W. S. Cassels, Lectures on elliptic curves, London Mathematical Society Student Texts, vol. 24, Cambridge University Press, Cambridge, 1991.

John E. Cremona, Algorithms for modular elliptic curves, 2nd ed., Cambridge University Press, Cambridge, 1997.

Anthony W. Knapp, Elliptic curves, Mathematical Notes, vol. 40, Princeton University Press, Princeton, NJ, 1992.

Neal Koblitz, Introduction to elliptic curves and modular forms, Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1984.

Joseph H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.

Joseph H. Silverman and John Tate, Rational points on elliptic curves, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.

Lawrence C. Washington, Elliptic curves: Number theory and cryptography, 2nd ED. Discrete Mathematics and Its Applications, Chapman & Hall/CRC, 2008.

Horst G. Zimmer, Computational aspects of the theory of elliptic curves, Number theory and applications (Banff, AB, 1988) NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., vol. 265, Kluwer Acad. Publ., Dordrecht, 1989, pp. 279–324.

Reviews on PKC
- DH
- ElGamal
- Massey – Omura

Discrete Logarithms
- DL Attacks
- BSGS
- Pohlih–Hellmann
- DL records

Square roots

Reminder from Yesterday
- Points of finite order

Important Results
- Hasse's Theorem
- Waterhouse's Theorem
- Rück's Theorem

Legendre Symbols

Further reading