

Elliptic and Hyperelliptic Curve Cryptography

An Introduction

Dr. F. Vercauteren

Katholieke Universiteit Leuven

10 June 2005

Elliptic Curves

Definition

Group Law

Hyperelliptic Curves

Definition

Group Law

DLP on Elliptic and Hyperelliptic Curves

Definition

Security

EC Cryptographic Primitives

Overview

Example: ECDSA

Elliptic Curves

Definition

- ▶ Elliptic curve E over field \mathbb{K} is defined by

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

- ▶ The set of \mathbb{K} -rational points $E(\mathbb{K})$ is defined as

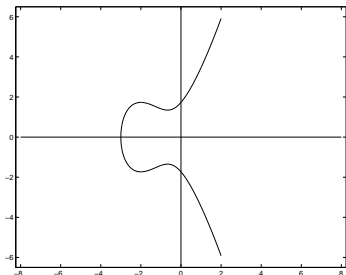
$$E(\mathbb{K}) = \{(x, y) \in \mathbb{K} \times \mathbb{K} \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\infty\}$$

- ▶ ∞ is called *point at infinity*

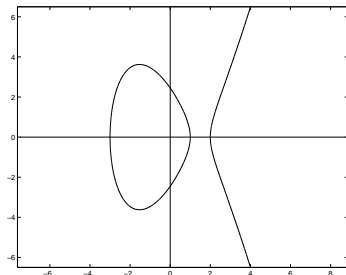
Theorem

There exists an addition law on E and the set $E(\mathbb{K})$ is a group

Elliptic Curves over \mathbb{R}

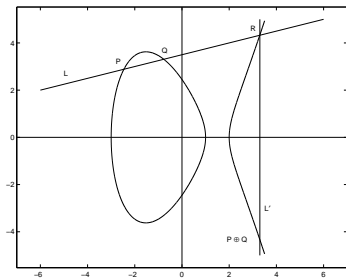


$$y^2 = x^3 + 4x^2 + 4x + 3$$

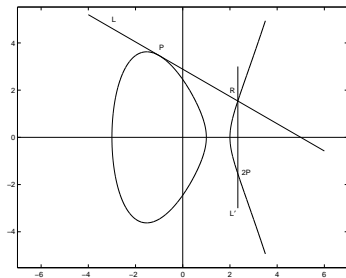


$$y^2 = x^3 - 7x + 6$$

Addition Law on Elliptic Curves



Adding two points



Doubling a point

$$y^2 = x^3 - 7x + 6$$

Addition Law on Elliptic Curves

By definition: three points on a line sum to zero!

Let $P_1 \oplus P_2 = P_3$, with $P_i = (x_i, y_i) \in E$

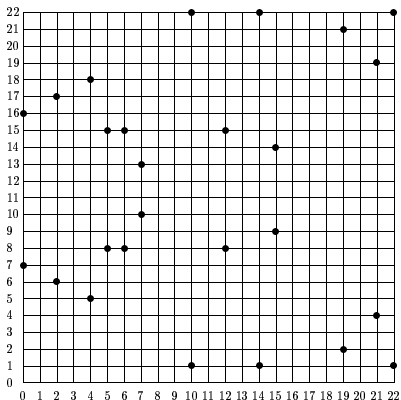
- ▶ If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$, then $P_1 \oplus P_2 = \infty$,
- ▶ Else

$$\begin{array}{l}
 x_1 \neq x_2 \\
 x_1 = x_2
 \end{array}
 \begin{cases}
 \lambda = (y_2 - y_1)/(x_2 - x_1) \\
 \nu = (y_1x_2 - y_2x_1)/(x_2 - x_1) \\
 \lambda = (3x_1^2 + 2a_2x_1 + a_4 - a_1y_1)/(2y_1 + a_1x_1 + a_3) \\
 \nu = (-x_1^3 + a_4x_1 + 2a_6 - a_3y_1)/(2y_1 + a_1x_1 + a_3)
 \end{cases}$$

The point $P_3 = P_1 \oplus P_2$ is given by

$$\begin{aligned}
 x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\
 y_3 &= -(\lambda + a_1)x_3 - \nu - a_3
 \end{aligned}$$

Elliptic Curves over Finite Fields



The elliptic curve $y^2 = x^3 + x + 3 \pmod{23}$

Hyperelliptic Curves

Definition

- ▶ Hyperelliptic curve H over field \mathbb{K} is defined by

$$y^2 + h(x)y = f(x) \quad h(x), f(x) \in \mathbb{K}[x]$$

with $\deg(h(x)) \leq g$ and $\deg(f(x)) = 2g + 1$

- ▶ $g \in \mathbb{N}$ is called the genus of H
- ▶ The set of \mathbb{K} -rational points on H is defined as

$$H(\mathbb{K}) := \{(x, y) \in \mathbb{K} \times \mathbb{K} \mid y^2 + h(x)y = f(x)\} \cup \{\infty\}$$

- ▶ For $\text{Char}(\mathbb{K}) > 2$, can take $h(x) = 0$

Note: elliptic curves are hyperelliptic curves of genus 1

Addition Law on Hyperelliptic Curve

- ▶ When $g \geq 2$, the points $H(\mathbb{K})$ do not form a group!
- ▶ Need to work with \mathbb{K} -rational points on Jacobian $J_H(\mathbb{K})$
- ▶ By definition: $J_H(\mathbb{K})$ is the smallest group in which $H(\mathbb{K})$ embeds, i.e. $H(\mathbb{K}) \subsetneq J_H(\mathbb{K})$
- ▶ For elliptic curves: $E(\mathbb{K}) \simeq J_E(\mathbb{K})$
- ▶ Generalisation of group law on elliptic curve: zeros of a polynomial sum to zero
- ▶ $\#J_H(\mathbb{F}_q) \simeq q^g$ for genus g hyperelliptic curve over \mathbb{F}_q

Construction of Jacobian

- ▶ Let \mathbb{F}_q be a finite field with $q = p^n$
- ▶ Let $\overline{\mathbb{F}}_q = \bigcup_{k=1}^{\infty} \mathbb{F}_{q^k}$ be its algebraic closure
- ▶ A divisor on H is finite formal sum

$$D = \sum_i m_i [P_i], \text{ with } P_i \in H(\overline{\mathbb{F}}_q)$$

- ▶ Set of all divisors is denoted $\text{Div}_H(\overline{\mathbb{F}}_q)$
- ▶ Degree of D is $\sum_i m_i$, $\text{Div}_H^0(\overline{\mathbb{F}}_q) =$ degree zero divisors
- ▶ For $P = (x, y)$ let $P^\sigma = (x^q, y^q)$ and $D^\sigma = \sum_i m_i [P_i^\sigma]$
- ▶ D is called \mathbb{F}_q -rational if $D^\sigma = D$
- ▶ For $P = (x, y)$, define the opposite as $-P = (x, -y - h(x))$

Construction of Jacobian

- ▶ Let $F(x, y) \in \mathbb{F}_q[x, y]$ be a polynomial and define

$$\text{Div}(F(x, y)) = \sum \text{ord}_P(F(x, y))[P] - (*)[\infty]$$

- ▶ $\text{ord}_P(F(x, y))$ measures order of vanishing at P
- ▶ $(*)$ chosen such that degree is zero
- ▶ Define for rational function $F(x, y)/G(x, y)$ the divisor

$$\text{Div}(F/G) = \text{Div}(F) - \text{Div}(G)$$

- ▶ These are called the principal divisors $P_H(\overline{\mathbb{F}}_q)$

Definition

The \mathbb{F}_q -rational points on the Jacobian of H are defined as

$$J_H(\mathbb{F}_q) = \text{Div}_H^0(\mathbb{F}_q) / (P_H(\mathbb{F}_q))$$

Computing in Jacobian

Definition

A divisor $D = \sum m_i [P_i] - (*)\infty \in \text{Div}_H^0$ is called **reduced** if:

1. All $m_i \geq 0$ and $m_i \leq 1$ if P_i is equal to its opposite
2. If $P_i \neq -P_i$, then only one of them occurs in the sum
3. $\sum m_i \leq g$

Theorem

Every element in $J_H(\mathbb{F}_q)$ can be uniquely represented by a reduced divisor

Mumford Representation

- ▶ Let $D = \sum m_i [P_i] - (*)\infty$ be reduced with $P_i = (x_i, y_i)$
- ▶ Define $u(x) = \prod_i (x - x_i)^{m_i}$ and $v(x)$ such that

$$v(x_i) = y_i$$

- ▶ Choose $\deg(v) < \deg(u) \leq g$ and

$$u(x) \mid v(x)^2 + h(x)v(x) - f(x)$$

- ▶ $(u(x), v(x))$ is called Mumford representation of D
- ▶ Can add two such representations using Cantor's algorithm
- ▶ For small genus: explicit formulae

Cantor's algorithm

Input: Divisors $D_1 = [u_1, v_1]$ and $D_2 = [u_2, v_2]$

Output: A divisor D representing the sum $D_1 + D_2$ in $J_C(\mathbb{F}_q)$

1. $d_1 = \gcd(u_1, u_2) = e_1 u_1 + e_2 u_2$
2. $d = \gcd(d_1, v_1 + v_2 + h) = c_1 d_1 + c_2 (v_1 + v_2 + h)$
3. $s_1 = c_1 e_1, s_2 = c_1 e_2, s_3 = c_2$
4. $u = (u_1 u_2) / d^2, v = (s_1 u_1 v_2 + s_2 u_2 v_1 + s_3 (v_1 v_2 + f)) / d \pmod u$
5. $u' = (f - v h - v^2) / u, v' = (-h - v) \pmod{u'}$
6. If $\deg(u') > g$ then $u = u', v = v',$ goto 5
7. Make u' monic by dividing it by its leading coefficient
8. Output $D = [u', v']$.

Elliptic and Hyperelliptic Curve DLP

- ▶ Let G be an abelian group generated by $P \in G$
- ▶ Let $Q = s \cdot P$, then the DLP is to compute s given P and Q
- ▶ Classically: $G = \mathbb{F}_q^\times$
- ▶ For $G = E(\mathbb{F}_q)$, the DLP is called ECDLP
- ▶ For $G = J_H(\mathbb{F}_q)$, the DLP is called HECDLP

Note: can translate primitives based on DLP to ECDLP and HECDLP setting

Security of ECDLP/HECDLP: General Attacks

- ▶ Exhaustive search: impossible if group order $> 2^{80}$
- ▶ Pohlig-Hellman: suppose $\#J_H(\mathbb{F}_q) = p_1^{s_1} \cdot p_2^{s_2} \cdot \dots \cdot p_k^{s_k}$, then can reduce HECDLP to subgroups of order p_i
 $\Rightarrow \#J_H(\mathbb{F}_q)$ should have large prime divisor p
- ▶ Pollard rho & lambda: random walk, constant space, time complexity is $O(\sqrt{N})$

Conclusion:

- ▶ $\#J_H(\mathbb{F}_q)$ should be at least 2^{160} and divisible by large prime p
- ▶ Best general attack is *exponential* in p

Security of ECDLP: Specific Attacks

Let r be largest prime factor of $\#J_H(\mathbb{F}_q)$ then:

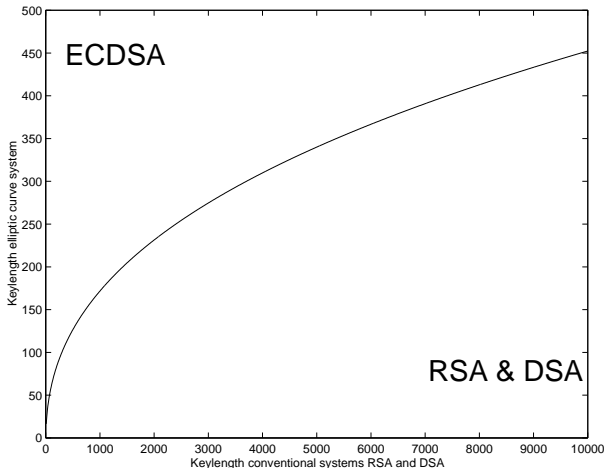
- ▶ Index calculus attack: if genus of H is > 2 , then index calculus applies and is faster than Pollard-Rho
- ▶ Multiplicative reduction: reduce HECDLP on $J_H(\mathbb{F}_q)$ to DLP in $\mathbb{F}_{q^k}^\times$, with k smallest integer with $q^k \equiv 1 \pmod r$,
- ▶ Additive reduction: if $r = p$, then HECDLP can be mapped to $\mathbb{F}_p, +$, and thus trivial to solve
- ▶ Weil descent: if H is defined over \mathbb{F}_{q^e} , then sometimes possible to find curve X over \mathbb{F}_q with $J_H(\mathbb{F}_{q^e}) \hookrightarrow J_X(\mathbb{F}_q)$, and apply index calculus in $J_X(\mathbb{F}_q)$

Security of ECDLP/HECDLP: Good Curves

Conclusion:

- ▶ Let \mathbb{F}_q with $q = p$ prime or $q = p^n$ with n prime
- ▶ Genus of H is either 1 or 2
- ▶ Let r be largest prime factor of $\#J_H(\mathbb{F}_q)$ then:
 - ▶ $r > 2^{160}$
 - ▶ $p \nmid r$
 - ▶ Smallest k with $q^k \equiv 1 \pmod{r}$ is > 50
 - ▶ Efficiency: require $\#J_H(\mathbb{F}_q)/r$ to be small

Comparison with RSA & DSA: Security



Key lengths in bits for equivalent cryptographic strength

Overview

- ▶ **Key Agreement Primitives**
 - ▶ ECDH: EC Diffie-Hellman Secret Value Derivation
 - ▶ ECMQV: EC Menezes-Qu-Vanstone Secret Value Derivation
- ▶ **Signature Primitives**
 - ▶ ECNR: EC Nyberg-Rueppel Signatures
 - ▶ ECDSA: EC Digital Signature Algorithm
- ▶ **Encryption Primitives**
 - ▶ ECIES: EC Integrated Encryption Scheme

EC Digital Signature Algorithm (ECDSA)

- ▶ **ECDSA** is elliptic curve analog of DSA
- ▶ Used to provide data origin authentication, data integrity and non-repudiation
- ▶ Standards for ECC (including ECDSA & ECIES):
 - ▶ ANSI X9.62, X9.63
 - ▶ NIST FIPS 186-2
 - ▶ IEEE 1363-2000
 - ▶ ISO/IEC 14888-3, 9796-4, 15946
 - ▶ SECG

EC Key Pair Generation

▶ Domain parameters

- ▶ Elliptic curve E over finite field \mathbb{F}_q
- ▶ Point $G \in E(\mathbb{F}_q)$, $n = \text{ord}(G)$ and cofactor $h = \#E(\mathbb{F}_q)/n$

▶ Private and public key

- ▶ Select random integer d in the interval $[1, n - 1]$
- ▶ Compute $Q = d \cdot G$
- ▶ **Public key** is Q , **Private key** is d

ECDSA Signature Generation

To sign a message m do the following:

1. Select a random integer k with $1 \leq k \leq n - 1$
2. Compute $k \cdot G = (x_1, y_1)$ and $r \equiv x_1 \pmod n$. If $r = 0$ go to step 1
3. Compute $k^{-1} \pmod n$
4. Compute $e = \text{HASH}(m)$
5. Compute $s \equiv k^{-1}(e + dr) \pmod n$. If $s = 0$ go to step 1
6. The signature for the message m is (r, s)

ECDSA Signature Verification

To verify a signature (r, s) on m do the following:

1. Verify that r and s are integers in the interval $[1, n - 1]$
2. Compute $e = \text{HASH}(m)$
3. Compute $w \equiv s^{-1} \pmod{n}$
4. Compute $u_1 \equiv ew \pmod{n}$ and $u_2 \equiv rw \pmod{n}$
5. Compute $u_1 \cdot G + u_2 \cdot Q = (x_1, y_1)$ and $v \equiv x_1 \pmod{n}$
6. Accept signature if and only if $v = r$

ECDSA vs. RSA: Speed (ms)

| | Elliptic curve over $\mathbb{F}_{2^{233}}$ | | |
|------------------------------------|--------------------------------------------|-----------|------------|
| | RIM pager | PalmPilot | Pentium II |
| Key Generation | 1,552 | 2,573 | 3.11 |
| ECDSA Signing | 1,910 | 3,080 | 4.03 |
| ECDSA Verifying | 3,701 | 5,878 | 7.87 |
| | 2048-bit modulus | | |
| | RIM pager | PalmPilot | Pentium II |
| RSA Key Generation | — | — | 26,442 |
| RSA Signing | 111,956 | 288,236 | 440.69 |
| RSA Verifying ($e = 3$) | 1,087 | 2,392 | 4.2 |
| RSA Verifying ($e = 2^{16} + 1$) | 3,608 | 7,973 | 13.45 |

More info: Brown et al.: PGP in Constrained Wireless Devices

Conclusions

- ▶ (Hyper)elliptic curves provide an alternative to RSA & DSA
- ▶ No sub-exponential time algorithm to solve HECDLP
- ▶ Smaller key sizes, sometimes faster than DSA & RSA, more future proof
- ▶ Typical applications: PDA's, phones, smart cards, ...