Elliptic Curve Cryptography

An Introduction

Dr. F. Vercauteren

Katholieke Universiteit Leuven

22 April 2008
Cryptography

Elliptic Curves

EC Cryptographic Primitives

Pairings
Cryptography provides the technical means to secure information in electronic form.

- **Confidentiality**: protection of data from unauthorized disclosure.
- **Data integrity**: assurance that data received are exactly as sent by an authorized entity.
- **Authentication**: assurance that the communicating entity is the one that it claims to be.
- **Non-repudiation**: prevents an entity from denying previous commitments or actions.
Symmetric Key Cryptography

\[
\text{ALICE} \quad \text{PLAINTEXT} \quad 110100011100 \\
\text{BOB} \quad \text{PLAINTEXT} \quad 110100011100 \\
\text{CIPHERTEXT} \quad ?????????????
\]

\[
\text{ENCRYPTION KEY} \quad = \quad \text{DECRIPTION KEY}
\]

Dr. F. Vercauteren
Elliptic Curve Cryptography An Introduction
Public Key Cryptography

ALICE

PUBLIC LIST

BOB

PUBLIC KEY CRYPTO SYSTEM

ENCRIPTION KEY

CIPHERTEXT

PLAINTEXT 110100011100

PUBLIC KEY OF BOB

PRIVATE KEY OF BOB

CIPHERTEXT ????

PLAINTEXT 110100011100

ENCRYPTION KEY

DECRYPTION KEY
Factoring and Discrete Logarithm Problem

  - Main idea: easy to find two large primes \( p \) and \( q \), but very hard to find \( p \) and \( q \) from \( n = p \cdot q \).
  - RSA still most popular public key cryptosystem.

  - Group \( G \) is set with operation \( \cdot \) and each element has inverse.
  - Main idea: very easy to compute \( h = g^x \) for given \( x \), but very hard to find \( x \) given \( h \) and \( g \).
  - Popular choices: finite fields and elliptic curves.
Diffie-Hellman Key Agreement

Choose a large prime number $p$ and a generator $\alpha \mod p$

\[
\begin{align*}
\text{Alice} & : x_A \in_R [1, p - 1], \alpha^{x_A} \\
\text{Bob} & : x_B \in_R [1, p - 1], \alpha^{x_B}
\end{align*}
\]

\[
K_{BA} = (\alpha^{x_B})^{x_A}
\]

- Note: all calculations mod $p$
- Security based on Diffie-Hellman problem: given $\alpha^{x_A}$ and $\alpha^{x_B}$ compute $\alpha^{x_Ax_B}$
Elliptic Curves

Definition

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

  $$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \ a_i \in \mathbb{K}$$

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

  $$E(\mathbb{K}) = \{(x, y) \in \mathbb{K} \times \mathbb{K} \mid y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6\} \cup \{\infty\}$$

- $\infty$ is called \textit{point at infinity}

Theorem

\textit{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 \( y_1 + y_2 + a_1 x_2 + a_3 = 0 \), then \( P_1 \oplus P_2 = \infty \),
- Else

\[
\begin{align*}
\lambda &= \frac{y_2 - y_1}{x_2 - x_1} \\
\nu &= \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}
\end{align*}
\]

\[
\begin{align*}
\lambda &= \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3} \\
\nu &= \frac{-x_1^3 + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3}
\end{align*}
\]

The point \( P_3 = P_1 \oplus P_2 \) is given by

\[
\begin{align*}
x_3 &= \lambda^2 + a_1 \lambda - a_2 - x_1 - x_2 \\
y_3 &= -(\lambda + a_1)x_3 - \nu - a_3
\end{align*}
\]
Finite Fields

- Practical applications need exact arithmetic, so
  - not $\mathbb{R}$ since not exact
  - not $\mathbb{Q}$ since size of numbers involved grows too fast
- Consider elliptic curves over finite fields:
  - $\mathbb{F}_p$ with $p$ prime: represented by $\mathbb{Z} \mod p$
  - $\mathbb{F}_{2^n}$ with $2^n$ elements: represented by $\mathbb{F}_2[X] \mod P(X)$, i.e. binary polynomials modulo an irreducible polynomial $P(X)$
Elliptic Curves over Finite Fields

The elliptic curve $y^2 = x^3 + x + 3 \mod 23$
Number of Points on Elliptic Curve

- Theorem: the cardinality $\#E(\mathbb{F}_q)$ satisfies
  $$\#E(\mathbb{F}_q) = q + 1 - t$$
  with $|t| \leq 2\sqrt{q}$.
- For $\gcd(q, t) = 1$, all possibilities occur.
Elliptic 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

Note: can translate primitives based on DLP to ECDLP setting
Security of ECDLP: General Attacks

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

**Conclusion:**

- $\#E(\mathbb{F}_q) > 2^{160}$ and divisible by large prime $p$
- Best general attack is exponential in $p$
- DLP in $\mathbb{F}_q$ is sub-exponential: $L_q[1/3, b]$ with

$$L_N[a, b] = O\left(e^{(b+O(1))(\ln N)^a(\ln \ln N)^{1-a}}\right)$$
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
Pairings

- Let $G_1$, $G_2$, $G_T$ be groups of prime order $\ell$. A pairing is a non-degenerate bilinear map $e : G_1 \times G_2 \rightarrow G_T$.
- Bilinearity:
  - $e(g_1 + g_2, h) = e(g_1, h)e(g_2, h)$,
  - $e(g, h_1 + h_2) = e(g, h_1)e(g, h_2)$.
- Non-degenerate:
  - for all $g \neq 1$: $\exists x \in G_2$ such that $e(g, x) \neq 1$
  - for all $h \neq 1$: $\exists x \in G_1$ such that $e(x, h) \neq 1$
- Examples:
  - Scalar product on vectorspace over finite fields
    \[
    \langle \cdot, \cdot \rangle : \mathbb{F}_q^n \times \mathbb{F}_q^n \rightarrow \mathbb{F}_q.
    \]
  - Weil- and Tate pairings on elliptic curves and abelian varieties.
Pairings in cryptography

- Exploit bilinearity: original schemes $G_1 = G_2$
  - MOV: DLP reduction from $G_1$ to $G_T$
    
    DLP in $G_1 : (g, xg) \Rightarrow$ DLP in $G_T : (e(g, g), e(g, g)^x)$
  
  - Decision DH easy in $G_1$
    
    DDH : $(g, ag, bg, cg)$ test if $e(g, cg) = e(ag, bg)$

- Identity based crypto, short signatures, ...
Torsion subgroups

- $E[\ell]$ subgroup of points of order dividing $\ell$, i.e.

$$E[\ell] = \{ P \in E(\overline{F}_q) | [\ell]P = \infty \}$$

- Structure of $E[\ell]$ for $\gcd(\ell, q) = 1$ is $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$.

- Let $\ell \nmid \#E(F_q)$, then $E(F_q)[\ell]$ gives at least one component.

- Embedding degree: $k$ minimal with $\ell \mid (q^k - 1)$.

- Note $\ell$-roots of unity $\mu_\ell \subseteq F_{q^k}^\times$.

- If $k > 1$ then $E(F_{q^k})[\ell] = E[\ell]$. 
Consider the function \( f = \frac{(x-1)^2(x+2)}{x} \) on \( \mathbb{P}^1 \)

▶ Divisor of \( f \): \( (f) = 2(P_1) + (P_{-2}) - (P_0) - 2(P_{\infty}) \)

▶ Support of \( (f) \): \( \text{Supp}((f)) = \{ P_1, P_{-2}, P_0, P_{\infty} \} \)

▶ Given divisor \( (f) \), function is determined up to constant.
Miller functions

- Let $P \in E(\mathbb{F}_q)$ and $n \in \mathbb{N}$.
- A Miller function $f_{n,P}$ is any function in $\mathbb{F}_q(E)$ with divisor
  \[
  (f_{n,P}) = n(P) - ([n]P) - (n - 1)(\infty)
  \]
- $f_{n,P}$ is determined up to a constant $c \in \mathbb{F}_q^\times$.
- $f_{n,P}$ has a zero at $P$ of order $n$.
- $f_{n,P}$ has a pole at $[n]P$ of order 1.
- $f_{n,P}$ has a pole at $\infty$ of order $(n - 1)$.
- For every point $Q \neq P, [n]P, \infty$, we have $f_{n,P}(Q) \in \mathbb{F}_q^\times$. 
Let $P \in E(\mathbb{F}_{q^k})[\ell]$ and $f_{\ell,P} \in \mathbb{F}_{q^k}(E)$ with

$$
(f_{\ell,P}) = \ell(P) - \ell(\infty)
$$

Note: $f_{\ell,P}$ has zero of order $\ell$ at $P$ and pole of order $\ell$ at $\infty$.

Tate pairing is defined as (assuming normalisation)

$$
\langle P, Q \rangle_\ell = f_{\ell,P}(Q)
$$

Technical stuff: need to adjust domain and image

$$
\langle \cdot, \cdot \rangle_\ell : E(\mathbb{F}_{q^k})[\ell] \times E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^\times / (\mathbb{F}_{q^k}^\times)^{\ell}
$$
Reduced Tate pairing

By definition, value of $\langle \cdot, \cdot \rangle_\ell$ only defined up to $\ell$-th powers.

$$\langle \cdot, \cdot \rangle_\ell : E(\mathbb{F}_{q^k})[\ell] \times E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k}) \rightarrow \mathbb{F}_{q^k}^\times / (\mathbb{F}_{q^k}^\times)^\ell$$

In practice: want unique output of the function!

Reduced Tate pairing $e : E(\mathbb{F}_{q^k})[\ell] \times E(\mathbb{F}_{q^k})/\ell E(\mathbb{F}_{q^k}) \rightarrow \mu_\ell$

$$e(P, Q) = \langle P, Q \rangle_\ell (q^k-1)/\ell = f_{\ell,P}(Q)(q^k-1)/\ell$$

Tate pairing is bilinear and non-degenerate.
Miller’s Algorithm

- Use double-add algorithm to compute $f_{n,P}$ for any $n \in \mathbb{N}$.
- Exploit relation:

\[ f_{m+n,P} = f_{m,P} \cdot f_{n,P} \cdot \frac{l_{[n]P,[m]P}}{v_{[n+m]P}} \]

- $l_{[n]P,[m]P}$: the line through $[n]P$ and $[m]P$
- $v_{[n+m]P}$: the vertical line through $[n + m]P$
- Evaluate at $Q$ in every step
Conclusions

- Elliptic curves provide an alternative to RSA & DSA
- No sub-exponential time algorithm to solve ECDLP
- Smaller key sizes, sometimes faster than DSA & RSA, more future proof
- Typical applications: PDA’s, phones, smart cards, …
- Examples: Blackberry, Wii, German passports, future EMV
- Pairings on elliptic curves: identity based crypto, short signatures, …
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 $r \equiv x_1 \mod n$. If $r = 0$ go to step 1
3. Compute $k^{-1} \mod n$
4. Compute $e = \text{HASH}(m)$
5. Compute $s \equiv k^{-1}(e + dr) \mod n$. 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 \(w \equiv s^{-1} \mod n\)
4. Compute \(u_1 \equiv ew \mod n\) and \(u_2 \equiv rw \mod n\)
5. Compute \(u_1 \cdot G + u_2 \cdot Q = (x_1, y_1)\) and \(v \equiv x_1 \mod n\)
6. Accept signature if and only if \(v = r\)
## ECDSA vs. RSA: Speed (ms)

<table>
<thead>
<tr>
<th></th>
<th>Elliptic curve over $\mathbb{F}_{2^{233}}$</th>
<th>2048-bit modulus</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RIM pager</td>
<td>PalmPilot</td>
</tr>
<tr>
<td>Key Generation</td>
<td>1,552</td>
<td>2,573</td>
</tr>
<tr>
<td>ECDSA Signing</td>
<td>1,910</td>
<td>3,080</td>
</tr>
<tr>
<td>ECDSA Verifying</td>
<td>3,701</td>
<td>5,878</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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