Curve-Based Cryptography

Nicolas Thériault
nicolas.theriault@usach.cl

Departamento de Matemática y Ciencia de la Computación
Universidad de Santiago de Chile
Computational Diffie-Hellman Problem: Given $g_1$, $[a]g_1$, and $[b]g_1$, compute $[ab]g_1$.

For a generic (additive) group $G$ and for well chosen values of $a$ et $b$, the fastest known method consists in solving the discrete log problem.
Computational Diffie-Hellman Problem: Given $g_1$, $[a]g_1$, and $[b]g_1$, compute $[ab]g_1$.

For a generic (additive) group $G$ and for well chosen values of $a$ et $b$, the fastest known method consists in solving the discrete log problem.

Given two elements $g_1$ and $g_\lambda$ of a group $G$ such that $g_\lambda \in \langle g_1 \rangle$, the **discrete logarithm problem** for the pair $(g_1, g_\lambda)$ in $G$ consist in computing the smallest positive integer $\lambda$ such that $g_\lambda = [\lambda]g_1$.

The security of many public key cryptosystems relies on the difficulty of the discrete log.
Three main types of attack:

- Shank’s Baby Step - Giant Step algorithm;
- Pollard’s $\rho$ method;
- Pollard’s kangaroo method.

They work for every abelian group.

They require

$$O \left( \sqrt{\text{group order}} \right)$$

group operations to solve the discrete log.
Example: Pollard’s ρ
For cryptographic applications, we would like square root algorithms to be the best possible attacks.
For cryptographic applications, we would like square root algorithms to be the best possible attacks. For some groups, it’s false:

- The additive group $\mathbb{Z}/p\mathbb{Z}$ (we can divide by $g_1$).
- Groups that decompose into small subgroups.
For cryptographic applications, we would like square root algorithms to be the best possible attacks. For some groups, it’s false:

➢ The additive group $\mathbb{Z}/p\mathbb{Z}$ (we can divide by $g_1$).
➢ Groups that decompose into small subgroups.

For others, it seems true (most of the time):

➢ Elliptic curves (of prime order).
➢ Hyperelliptic curves of genus 2 (of prime order).
For cryptographic applications, we would like square root algorithms to be the best possible attacks. For some groups, it’s false:

- The additive group $\mathbb{Z}/p\mathbb{Z}$ (we can divide by $g_1$).
- Groups that decompose into small subgroups.

For others, it seems true (most of the time):

- Elliptic curves (of prime order).
- Hyperelliptic curves of genus 2 (of prime order).

For others, it’s false, but not too much:

- Hyperelliptic curves of genus 3 and 4.
- Non-hyperelliptic curves of genus 4.
Curve:

➤ Has an equation of the form $y^2 = x^3 + ax + b$
  (Weierstrass form)

➤ over a field of $q$ elements, $q = p^k$.

➤ such that $4a^3 + 27b^2 \neq 0 \text{ mod } p$ (non-singular)

Group:

➤ The (affine) rational points on the curve of the form
  $(x_i, y_i)$ where $y_i^2 = x_i^3 + ax_i + b$

➤ an extra point “at infinity”, $P_\infty$, which will be the
  zero/neutral of the group

➤ a group operation between pairs of points
\[ y^2 = x^3 - x \]
Point Addition for $E(\mathbb{R})$

\[
y^2 = x^3 - x
\]
$y^2 = x^3 - x$
Point Addition for $E(\mathbb{R})$

$y^2 = x^3 - x$
Group operation

Special cases:

- two distinct points on the same vertical add to $P_\infty$
- if the $y$-coordinate is 0, the double of the point is $P_\infty$
- adding $P_\infty$ to any point returns the same point

General case, the chord-and-tangent method:

- $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$
- $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = -y_1 - \lambda(x_3 - x_1)$
- $\lambda$ is the slope of the line between the two initial points (of the tangent if both points are the same)
- $\lambda = \frac{y_1-y_2}{x_1-x_2}$ (general addition) or $\frac{3x_1^2+a}{2y_1}$ (doubling)
There are other ways to represent elliptic curves, which can give different group operations.

A popular representation is Edwards curves:
\[ x^2 + y^2 = 1 - dx^2y^2 \]

Projective coordinates: represent points as triples (or more) of coordinates, to avoid field divisions.

Maps:

- The complete (extended) group should include all points over the algebraic closure of the field.
- Isomorphisms: to change the equation but keep the exact same group.
- Isogenies: maps between curves with a finite kernel.
Hyperelliptic Curves

A hyperelliptic curve \( C \) of genus \( g \) is defined by an equation of the form:

\[
C : Y^2 + h(X)Y = f(X)
\]

with

\[
\begin{align*}
\text{deg}(h) & \leq g; \\
\text{deg}(f) & = 2g + 1;
\end{align*}
\]

a tangent to the curve defined at every point.

Elliptic curves are hyperelliptic curves of genus 1.

In genus greater than 1, points do not form a group.
$y^2 = x^5 - 5x^4 - \frac{9}{4}x^3 + \frac{101}{4}x^2 + \frac{1}{2}x - 6$
HEC over $\mathbb{R}$, genus 2

\[ y^2 = x^5 - 5x^4 - \frac{9}{4}x^3 + \frac{101}{4}x^2 + \frac{1}{2}x - 6 \]
$y^2 = x^5 - 5x^4 - \frac{9}{4}x^3 + \frac{101}{4}x^2 + \frac{1}{2}x - 6$
HEC over $\mathbb{R}$, genus 2

$$y^2 = x^5 - 5x^4 - \frac{9}{4}x^3 + \frac{101}{4}x^2 + \frac{1}{2}x - 6$$
Divisor Class Group

Divisors (sums of points, including $\infty$) of degree zero ($\sum$ coefficients $= 0$) form an infinite additive group.

A principal divisor is the sum of the points of intersection between the curve and a polynomial in $x$ and $y$. Principal divisors are a normal subgroup of the divisors of degree zero.

The Jacobian is the group of divisor classes (i.e. divisors of degree zero modulo principal divisors).

A reduced divisor is the sum of at most $g$ points $(-\infty)$ and does not contain any pair of points $(x, y), (x, -y - h(x))$.

The element of the Jacobian of $C$ (the divisor classes) are represented by reduced divisors.
Going back to the genus 2 curve, with two divisors \((P_1 + P_2 - 2\infty)\) and \((Q_1 + Q_2 - 2\infty)\).
There exists a unique cubic which fits these four points.
The cubic intersects $C$ in two more points.
Jacobian Addition

We reflect these points with the $x$-axis and obtain:

$$(P_1 + P_2 - 2\infty) + (Q_1 + Q_2 - 2\infty) =$$

$$= R_1 + R_2 - 2\infty$$
Curve of Genus 4
Curve of Genus 4
Curve of Genus 4
Courbe de genre 3

\[ y^2 = x^7 + \frac{1}{2}x^6 - \frac{847}{144}x^5 - \frac{325}{144}x^4 + \frac{1763}{192}x^3 + \frac{403}{144}x^2 - \frac{1667}{576}x + \frac{35}{96} \]
On veut additionner les diviseurs

\[ D_1 = P_1 + P_2 + P_3 - 3\infty \]

et \[ D_2 = Q_1 + Q_2 + Q_3 - 3\infty \]
La première réduction n’est pas suffisante (on attend pour la réflexion avec l’axe des $x$).
On obtient:

\[ D_1 + D_2 = S_1 + S_2 + S_3 - 3\infty \]
We consider at the ring of polynomials

\[
R = \frac{\mathbb{F}_q[x, y]}{(y^2 + h(x)y - f(x))}
\]

and we look at ideals of this ring.

The ideal

\[
I = (p_1(x, y), p_2(x, y))
\]

is the set of all polynomials of the form

\[
r_1(x, y)p_1(x, y) + r_2(x, y)p_2(x, y) \mod (y^2 + h(x)y - f(x)).
\]

\(p_1\) and \(p_2\) are the generators of \(I\).
The ideals of $R$ form an infinite multiplicative group.

A principal ideal is an ideal with a single generator, for example $(y - 3x^2 + 8x - 4)$.

The principal ideals of $R$ are a normal subgroup of the ideals of $R$.

The ideal class group is the group:

$$\frac{\text{ideals of } R}{\text{principal ideals of } R}$$

This is a finite multiplicative group.
Ideal Classes

Each class of ideals contains a unique reduced ideal of the form

\[ I = (u(x), y - v(x)) \]

with \( \deg(u) \leq g \), \( u \) monic and \( \deg(v) < \deg(u) \).
(By construction, \( u(x) \) divides \( v(x)^2 + h(x)v(x) - f(x) \).)

For hyperelliptic curves, the ideal class group is isomorphic to the divisor class group \( (Jac(C)(\mathbb{F}_q)) \).

Working with the ideal class group is easier!!!
The group order of a curve of genus $g$ over a field of $q$ elements is:

$$|Jac(C)(\mathbb{F}_q)| = q^g + O(gq^{g-1/2}),$$

so to have the same group order as ECC, we divide the number of bits of the field order by $g$.

Field multiplications are then $\sim g^2$ times faster (and use less energy).

On the other hand, a group operation takes $O(g^2)$ field operations.

At a first glance, the difference should be small.
Composition

Input: ideals $I_1 = (u_1(x), y - v_1(x))$ and $I_2 = (u_2(x), y - v_2(x))$.

Output: ideal $I_C = (u_C(x), y - v_C(x))$ (not reduced).
Input: ideals $I_1 = (u_1(x), y - v_1(x))$ and $I_2 = (u_2(x), y - v_2(x))$.

1. $d_1 = s_1u_1 + s_2u_2 \leftarrow \gcd(u_1, u_2)$.
2. $d = t_1d_1 + t_2(v_1 + v_2 + h) \leftarrow \gcd(d_1, v_1 + v_2 + h_2)$.
3. $r_1 \leftarrow s_1t_1$, $r_2 \leftarrow s_2t_1$, and $r_3 \leftarrow t_2$.

Output: ideal $I_C = (u_C(x), y - v_C(x))$ (not reduced).
Input: ideals $I_1 = (u_1(x), y - v_1(x))$ and $I_2 = (u_2(x), y - v_2(x))$.

1. $d_1 = s_1u_1 + s_2u_2 \leftarrow \gcd(u_1, u_2)$.
2. $d = t_1d_1 + t_2(v_1 + v_2 + h) \leftarrow \gcd(d_1, v_1 + v_2 + h_2)$.
3. $r_1 \leftarrow s_1t_1$, $r_2 \leftarrow s_2t_1$, and $r_3 \leftarrow t_2$.
4. $u_C \leftarrow u_1u_2/d^2$.
5. $v_C \leftarrow v_2 + \frac{u_2}{d}r_2(v_1 + v_2) + r_3\frac{v_2^2 + hv_2 + f}{d}$.

Output: ideal $I_C = (u_C(x), y - v_C(x))$ (not reduced).
Input: ideal \( I_C = (u_C(x), y - v_C(x)) \).

Output: reduced ideal \( I_3 = (u_3(x), y - v_3(x)) \).
Input: ideal $I_C = (u_C(x), y - v_C(x))$.

1. $\tilde{u}_0 \leftarrow u_C, \tilde{v}_0 \leftarrow v_C$.

Output: reduced ideal $I_3 = (u_3(x), y - v_3(x))$. 
Input: ideal $I_C = (u_C(x), y - v_C(x))$.

1. $\tilde{u}_0 \leftarrow u_C$, $\tilde{v}_0 \leftarrow v_C$.
2. From $i = 0$, while $\deg(\tilde{u}_i) > g$:

Output: reduced ideal $I_3 = (u_3(x), y - v_3(x))$. 
Input: ideal $I_C = (u_C(x), y - v_C(x))$.

1. $\tilde{u}_0 \leftarrow u_C, \tilde{v}_0 \leftarrow v_C$.

2. From $i = 0$, while $\deg(\tilde{u}_i) > g$:
   
   (a) $\tilde{u}_{i+1} \leftarrow \text{Monic} \left( \frac{\tilde{v}_i^2 + h\tilde{v}_i + f}{\tilde{u}_i} \right)$.
   
   (b) $\tilde{v}_{i+1} \leftarrow \tilde{v}_i + h \mod \tilde{u}_{i+1}$.
   
   (c) $i \leftarrow i + 1$.

Output: reduced ideal $I_3 = (u_3(x), y - v_3(x))$. 
Input: ideal $I_C = (u_C(x), y - v_C(x))$.

1. $\tilde{u}_0 \leftarrow u_C, \tilde{v}_0 \leftarrow v_C$.

2. From $i = 0$, while $\text{deg}(\tilde{u}_i) > g$:
   
   (a) $\tilde{u}_{i+1} \leftarrow \text{Monic}\left(\frac{\tilde{v}_i^2 + h\tilde{v}_i + f}{\tilde{u}_i}\right)$.
   
   (b) $\tilde{v}_{i+1} \leftarrow \tilde{v}_i + h \mod \tilde{u}_{i+1}$.
   
   (c) $i \leftarrow i + 1$.

3. $u_3 \leftarrow \tilde{u}_i, v_3 \leftarrow \tilde{v}_i$.

Output: reduced ideal $I_3 = (u_3(x), y - v_3(x))$. 
Attacks for HEC

➤ Weil descent attack:
  ➤ Frey (1998), Gaudry–Hess–Smart (2000), ...
  ➤ Gaudry (2004)

➤ Index calculus attack for large genus:
  ➤ Adleman–DeMarrais–Huang (1999)
  ➤ Enge-Gaudry-Thomé (2009)

➤ Index calculus attack for small genus:
  ➤ Diem (2006): non-hyperelliptic curves
Curves and security

- Use isomorphisms to choose a form of the curve equation that reduces the cost of the group operation

- Assume the fastest known attack

- The secret key size (scalar) depends only on the security level, not the group order

<table>
<thead>
<tr>
<th>genus</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>fields size (bits)</td>
<td>n</td>
<td>n/2</td>
<td>3n/8</td>
<td>n/3</td>
</tr>
<tr>
<td>group size (bits)</td>
<td>n</td>
<td>n</td>
<td>9n/8</td>
<td>4n/3</td>
</tr>
<tr>
<td>key size (bits)</td>
<td>n</td>
<td>n</td>
<td>n</td>
<td>n</td>
</tr>
</tbody>
</table>
1. Work based on the coefficients instead of polynomials (explicit formulæ)

2. Combine inversions

3. Reduce the number of multiplications
   (a) Faster algorithms
   (b) Karatsuba-like tricks