Elliptic Curve Cryptography and the Anomalous Attack

Isik Ulusan

December 4, 2025

Discrete Logarithm Problem and Cryptography

Let F be a field and $g \in F$, $a \in \mathbb{Z}$. The Discrete Logarithm Problem (DLP) is the following: Given g^a and g, find a.

No efficient[1] solutions to the DLP are known.

Consequently a lot of cryptography, like Diffie-Hellman and its derivatives, are based on this difficulty of the DLP.

[1] No poly-time computable randomized algorithm is known.

Elliptic Curves

In practice the elliptic curves used are of the form $y^2 = x^3 + ax + b$ over a field F. For the rest of the time we will consider $F = \mathbb{F}_q$ for some q.

Importantly, elliptic curves are abelian varieties, so they have a group law. (The points on them behave like an abelian group.) As a result we can perform addition in some manner.

[BSS]

Algebraic Geometry Detour

Elliptic Curves are smooth projective varieties.

For our purposes, we can think of them living inside $\mathbb{A}^2 + \mathbb{P}^1 \cong \mathbb{P}^2$. Here $\mathbb{P}^1$ is the line at infinity, which can be thought of as infinitely far away from our plane $\mathbb{A}^2$.

For our elliptic curve $E \subseteq \mathbb{P}^2$, we will have a "point at infinity" $\mathcal{O}$ where $E \cap \mathbb{P}_1 = \{\mathcal{O}\}$.

[Reid]

Group Law

We define the group law for our elliptic curve E in the following:
The identity element is $\mathcal{O}$ and addition is defined as such:

- Any line L passing through E intersects at exactly 3 points (counting multiplicities and $\mathcal{O}$).
- The sum of these 3 points is always 0.
- Say $L \cap E = \{P, Q, R\}$ so $P + Q + R = 0$ and $P + Q = -R$.

The inverses just follow from that $P - P + \mathcal{O} = 0$. So inverses are just translations across the x-axis.

[BSS] and [Reid]

Elliptic Curve Discrete Logarithm Problem

From addition we can define multiplication by repeated additions, denoted as $[m]P$.

The Elliptic Curve Discrete Logarithm Problem is finding m, given $[m]P$ and P in E.

This is practically harder than DLP, so it can get away with shorter keys for the same security:

DLP	ECDLP
1024 bits	173 bits
4096 bits	313 bits

[BSS]

Anomalous Curves

Anomalous Curves are elliptic curves $E(\mathbb{F}_p)$ such that $p = \#E(\mathbb{F}_p)$. So the characteristic of the field is equal to the number of elements of the curve.

These were proposed to be used after super-singular curves were shown to be vulnerable to the MOV Attack. Anomalous curves are by definition, not super-singular.

Anomalous Curves are also resistant to traditional attacks such as BSGS and lambda-rho methods.

[BSS]

The Exact Sequences

The Anomalous Attack uses two exact sequences that relate to one another.

$$0 \longrightarrow E_1(\mathbb{Q}_p) \longrightarrow E_0(\mathbb{Q}_p) \longrightarrow E(\mathbb{F}_p) \longrightarrow 0 \qquad f : x \to x \bmod p$$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_2(\mathbb{Q}_p) & \longrightarrow & E_1(\mathbb{Q}_p) & \longrightarrow & \mathbb{F}_p^+ & \longrightarrow & 0 \\ & & \downarrow v_p & & \downarrow v_p & & \downarrow v_p & & \\ 0 & \longrightarrow & p^2\mathbb{Z}_p & \longrightarrow & p\mathbb{Z}_p & \longrightarrow & \mathbb{F}_p & \longrightarrow & 0 \end{array} \qquad f : x \to v_p$$

Here, $E_1(\mathbb{Q}_p)$ is the points in $E(\mathbb{Q}_p)$ that reduce to $(0 \bmod p, 0 \bmod p)$.
$E_2(\mathbb{Q}_p)$ is the points in $E(\mathbb{Q}_p)$ that reduce to (g, g'), where $g, g' \in \mathbb{F}_p$.
v_p is the p-adic elliptic logarithm: $v_p : (p, q) \to -p/q$.

The Anomalous Attack

- Let $Q = [m]P \in E(\mathbb{F}_p)$. Then compute the Hensel lifts to get $P - [m]Q = R \in E_1(\mathbb{Q}_p)$.
- Since the curve is anomalous: $\#E(\mathbb{F}_p) = \#\mathbb{F}_p^+$.
- $[p]P - [m]([p]Q) = [p]R \in E_2(\mathbb{Q}_p)$ since $R \in E_1(\mathbb{Q}_p)$. This can be seen from the diagram as $p\mathbb{Z}_p$ to $p^2\mathbb{Z}_p$.
- Now take the v_p: $v_p([p]P - [m]v_p([p]Q)) = v_p([p]R) \equiv 0 \mod p^2$.
- So $m \equiv v_p([p]P)/v_p([p]Q) \mod p$.

Importantly, the p-adic elliptic logarithm is efficiently computable, so m is also efficiently computable.

Showing that ECDLP is easy for anomalous curves.

[Smart]

References

[BSS] Blake, Seroussi, and Smart - Elliptic Curves in Cryptography.

[Reid] Reid - Undergraduate Algebraic Geometry.

[Smart] Smart - The Discrete Logarithm Problem on Elliptic Curves of Trace One.