Elliptic-curve cryptography XIII

Security requirements

Tanja Lange

Eindhoven University of Technology

2MMC10 – Cryptology

Summary of other attacks

Anomalous curves:
If $E/\mathbf{F}_p$ has $\#E(\mathbf{F}_p) = p$ then can transfer $E(\mathbf{F}_p)$ to $(\mathbf{F}_p, +)$.

Summary of other attacks

Anomalous curves:
If $E/\mathbf{F}_p$ has $\#E(\mathbf{F}_p) = p$ then can transfer $E(\mathbf{F}_p)$ to $(\mathbf{F}_p, +)$.
Very easy DLP.

Summary of other attacks

Anomalous curves:
If $E/\mathbf{F}_p$ has $\#E(\mathbf{F}_p) = p$ then can transfer $E(\mathbf{F}_p)$ to $(\mathbf{F}_p, +)$.
Very easy DLP.

Weil descent:
Maps DLP in E over $\mathbf{F}_{p^{mn}}$ to DLP on variety J over $\mathbf{F}_{p^n}$.

Summary of other attacks

Anomalous curves:
If $E/\mathbf{F}_p$ has $\#E(\mathbf{F}_p) = p$ then can transfer $E(\mathbf{F}_p)$ to $(\mathbf{F}_p, +)$.
Very easy DLP.

Weil descent:
Maps DLP in E over $\mathbf{F}_{p^{mn}}$ to DLP on variety J over $\mathbf{F}_{p^n}$.
Elements in J represented as polynomials of low'ish degree.
$\Rightarrow$ Can mount index calculus there.

This is efficient if dimension of J is not too big.

Summary of other attacks

Anomalous curves:
If $E/\mathbf{F}_p$ has $\#E(\mathbf{F}_p) = p$ then can transfer $E(\mathbf{F}_p)$ to $(\mathbf{F}_p, +)$.
Very easy DLP.

Weil descent:
Maps DLP in E over $\mathbf{F}_{p^{mn}}$ to DLP on variety J over $\mathbf{F}_{p^n}$.
Elements in J represented as polynomials of low'ish degree.
$\Rightarrow$ Can mount index calculus there.

This is efficient if dimension of J is not too big.

Particularly nice if J is Jacobian of hyperelliptic curve C.
For genus g index calculus with small poly takes $\tilde{O}(p^{2-\frac{2}{g+1}})$;
attack for $g > 3$.

Security requirements

We want elliptic curve $E/\mathbf{F}_p$ with

- $\#E(\mathbf{F}_p)$ almost prime, e.g., $\#E(\mathbf{F}_p) = 2^r \cdot \ell,\ r \leq 3$.
- $p \approx \ell$ of ≈ 256 bits.
- E should be ordinary, i.e., $\#E(\mathbf{F}_p) \neq p + 1$.
- E should not be anomalous, i.e., $\#E(\mathbf{F}_p) \neq p$.

These are concerns about ECDLP security.
Note: p, not p^n, so no Weil descent.

Security requirements

We want elliptic curve $E/\mathbf{F}_p$ with

- $\#E(\mathbf{F}_p)$ almost prime, e.g., $\#E(\mathbf{F}_p) = 2^r \cdot \ell,\ r \leq 3$.
- $p \approx \ell$ of ≈ 256 bits.
- E should be ordinary, i.e., $\#E(\mathbf{F}_p) \neq p + 1$.
- E should not be anomalous, i.e., $\#E(\mathbf{F}_p) \neq p$.

These are concerns about ECDLP security.
Note: p, not p^n, so no Weil descent.

For more properties and implementation security see
https://safecurves.cr.yp.to/