Weak instances of ECDLP

With a focus on finite local rings

D. Taufer
KU Leuven
July 26, 2023

1 Outline

1 DLP

Let G be a group, $P \in G$, $Q \in \langle P \rangle = \{0, P, 2P, 3P, \dots\}$.

Discrete logarithm problem (DLP)

Compute $n \in \mathbb{Z}$ such that $Q = nP$.

(Silly) example

$G = (\mathbb{R}^*, \cdot)$, $P = 10$, $Q = 1000$. As

$$Q = P \cdot P \cdot P \implies n = 3.$$

You figure it out by simply counting the digits of Q: (super) efficient!
$\rightsquigarrow$ not smart for constructing one-way functions.

KU LEUVEN

1 Crypto-why

Easy way to construct key-exchange protocols: $G = \langle g \rangle$, and

$$\begin{tikzcd}
\boxed{\text{Alice}} & \boxed{\text{Bob}} \\
a \in \mathbb{Z} \arrow[d] & b \in \mathbb{Z} \arrow[d] \\
g_a = g^a \in G \arrow[dr] & g_b = g^b \in G \arrow[dl] \\
g_{ab} = (g^b)^a \in G & g_{ab} = (g^a)^b \in G
\end{tikzcd}$$

1 Crypto-why

Easy way to construct key-exchange protocols: $G = \langle g \rangle$, and

Alice	Eve	Bob
$a \in \mathbb{Z}$		$b \in \mathbb{Z}$
$\downarrow$		$\downarrow$
$g_a = g^a \in G$	$g_a, g_b \overset{?}{\rightsquigarrow} g_{ab}$	$g_b = g^b \in G$
$g_{ab} = (g^b)^a \in G$		$g_{ab} = (g^a)^b \in G$

1 ECDLP

We usually employ $G =$ group of points of an elliptic curve E defined over a finite field.

Elliptic curve

Smooth plane projective cubic with a specified point $\mathcal{O}$.

... in practice

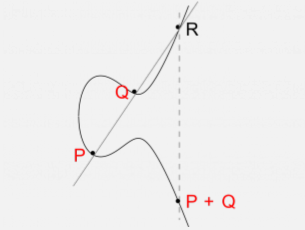
The projective points $(X : Y : Z) \in \mathbb{P}^2(\mathbb{F}_q)$ satisfying a Weierstrass equation

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

The specified point ("at infinity") is $\mathcal{O} = (0 : 1 : 0)$.

1 Point operation

Chord-tangent definition



... But can also be defined on open coverings!

W. Bosma, H. W. Lenstra, *Complete Systems of Two Addition Laws for Elliptic Curves*, J. Number Theory 53, 1995, pp. 229–240.

1 Elliptic curves over rings

Point operation

There are $f_x, f_y, f_z \in \mathbb{Z}[x_1, y_1, z_1, x_2, y_2, z_2]_{(2,2)}$ such that

$$(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2) =$$

$$(f_x(X_i, Y_i, Z_i) : f_y(X_i, Y_i, Z_i) : f_z(X_i, Y_i, Z_i)).$$

[Oversimplified]

In some cases, these f_*'s may also have "nice" representations.

M. Sala, D. Taufer, *Elliptic Loops*, J. Pure Appl. Algebra 227 (12), 2023.

1 Elliptic curves over rings

EC/Rings

It is possible to extend the group operation to rings with finitely many maximal ideals.
Over such rings, we can still define elliptic curves with an explicit projective description!

H. W. Lenstra, *Elliptic curves and number-theoretic algorithms*, Proc. International Congress of Mathematicians, 1986, pp. 99–120.

2 Outline

1. Introduction
2. Hardness of the ECDLP
3. ECDLP over rings
4. Take-home

2 Hardness of the ECDLP

The ECDLP is *usually* difficult over $\mathbb{F}_q$, i.e. the best-known algorithms (Baby-step Giant-step, Pollard rho/kangaroo) are exponential in the size of the input parameters ($\sim \mathrm{O}(\sqrt{q})$).

BUT

- We do not have proof of hardness.
- There are proven exceptions:
  - ECs with smooth orders.
  - (Sub)groups of order p^i, with $p|q$.
  - ECs with a small embedding degree.
  - ECs that may be (homomorphically) mapped into low-genus algebraic curves.
  - ECs over small degree extension fields.

2 Pohlig–Hellman

If P generates a group of order $N = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$, you solve many smaller ECDLP:

$$\begin{aligned}
\frac{N}{p_1} Q &= \lambda_1 \frac{N}{p_1} P, \\
\frac{N}{p_1^2} Q &= (\lambda_1 + \lambda_2 p_1) \frac{N}{p_1^2} P, \\
&\vdots \\
\frac{N}{p_1^{e_1}} Q &= (\lambda_1 + \lambda_2 p_1 + \ldots + \lambda_{e_1} p_1^{e_1 - 1}) \frac{N}{p_1^{e_1}} P.
\end{aligned}$$

This provides us with the logarithm modulo $p_1^{e_1}$.
Repeat for every $p_i^{e_i}$ and recover the complete logarithm via CRT.

2 Lifting the curve

If $\langle P \rangle$ is a p-group, the corresponding ECDLP may be read by lifting:

$$E(\mathbb{Z}/p^2\mathbb{Z}) \xrightarrow{\text{mod } p} E(\mathbb{F}_p),$$
$$P^{\uparrow}, Q^{\uparrow} \mapsto P, Q.$$

$$pP^{\uparrow} = (pX : 1 : 0), \quad pQ^{\uparrow} = (npX : 1 : 0).$$

T. Satoh, K. Araki, *Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves*, Comm. Math. Univ. Sancti Pauli 47, 1998, pp. 81–92.

N. Smart, *The discrete logarithm on elliptic curves of trace one*, J. Cryptology 12, 1999, pp. 193–196.

M. Sala, D. Taufer, *The group structure of elliptic curves over $\mathbb{Z}/N\mathbb{Z}$*,

ArXiv:2010.15543.

2 Pairings and MOV

Need a pairing

$$e : E(\mathbb{F}_q) \times E(\mathbb{F}_q) \to \mathbb{F}_{q^k}^*,$$

namely

- bilinear,
- non-degenerate,
- efficiently computable.

$$\rightsquigarrow e(Q, P) = e(nP, P) = e(P, P)^n,$$

Recover n by solving a DLP in $\mathbb{F}_{q^k}^*$.

A. Menezes, T. Okamoto, S. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, STOC '91: Proceedings of the twenty-third annual ACM symposium on Theory of Computing, 1991, pp. 80–89.

2 Weil descent

Need a hyperelliptic curve H and a computable group homomorphism

$$\phi : E(\mathbb{F}_{(2^m)^k}) \to \mathsf{Jac}_H.$$

If the genus of H is small ($\sim k$), the DLP on Jac_H may be (asymptotically) easier than the starting one:

$$\rightsquigarrow \text{solve} \quad \phi(Q) = \phi(nP) = n\phi(P).$$

P. Gaudry, F. Hess, N. Smart, *Constructive and destructive facets of Weil descent on elliptic curves*, J. Cryptology 15, 2002, pp. 19–46.

This occurs rarely!

F. Hess, *Weil descent attacks*, in *Advances in elliptic curve cryptography*, London Math. Soc. Lecture Note Ser. 317, Cambridge Univ. Press, 2005, pp. 151–180.

2 Index calculus for field towers

Need a factor base $\mathcal{F} = \{P_1, P_2, \ldots, P_r\}$ and relations

$$\alpha_1 Q + \beta_1 P = \sum_{P_i \in \mathcal{S}_1 \subset \mathcal{F}} P_i,$$

$$\alpha_2 Q + \beta_2 P = \sum_{P_i \in \mathcal{S}_2 \subset \mathcal{F}} P_i,$$

$$\vdots$$

$$\alpha_{r+1} Q + \beta_{r+1} P = \sum_{P_i \in \mathcal{S}_{r+1} \subset \mathcal{F}} P_i.$$

(huge) linear algebra $\rightsquigarrow \alpha Q + \beta P = 0 \implies n = -\frac{\beta}{\alpha}.$

I. A. Semaev, *Summation polynomials and the discrete logarithm problem on elliptic curves*, Cryptology ePrint Archive, Report 2004/031, 2004.

2 Index calculus for field towers

In practice: not effective in general, but works well for curves defined over field extensions: $\mathbb{F}_{q^k}$.

C. Diem, *On the discrete logarithm problem in elliptic curves*, Compos. Math. 147, 2011, pp. 75–104.

P. Gaudry, *Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem*, J. Symbolic Comput. 44, 2008, pp. 1690–1702.

We gain even more by applying it with special choices of factor bases combined with GB-methods!

A. Joux, V. Vitse, *Elliptic Curve Discrete Logarithm Problem over Small Degree Extension Fields*, J. Cryptology 26, 2013, pp. 119–143.

3 Outline

3 What about rings?

When $\gcd(p,q)=1$, we have

$$E(\mathbb{Z}/pq\mathbb{Z}) \simeq E(\mathbb{Z}/p\mathbb{Z}) \times E(\mathbb{Z}/q\mathbb{Z}),$$

while for prime powers we almost always have

$$E(\mathbb{Z}/p^e\mathbb{Z}) \simeq E(\mathbb{Z}/p\mathbb{Z}) \times \mathbb{Z}/p^{e-1}\mathbb{Z}.$$

The latter isomorphism is explicit and effective, hence we are not increasing the ECDLP difficulty w.r.t. $E(\mathbb{F}_p)$.

M. Sala, D. Taufer, *The group structure of elliptic curves over* $\mathbb{Z}/N\mathbb{Z}$, ArXiv:2010.15543.

3 More generally, for finite local rings

$(R, \mathfrak{m})$ local. The operations in the group at infinity

$$E^{\infty}(R) = \{\text{Points projecting to } \mathcal{O} \in E(R/\mathfrak{m}) \bmod \mathfrak{m}\}$$

are “easier than they should be”.

Corollary

Let $R = \mathbb{F}_q[x]/(x^k)$. The ECDLP over $E(R)$ is almost always polynomially equivalent to the ECDLP over $E(\mathbb{F}_q)$.

R. Invernizzi, D. Taufer, *Multiplication polynomials for elliptic curves over finite local rings*, ACM's International Conference Proceedings Series (ISSAC'23), 2023, pp. 335–344.

3 Multiplication Polynomials

Framework

Finite local ring $(R, \mathfrak{m})$, E elliptic curve over R. We look at the coordinate of nP when

$$P = (X' : Y' : Z') \in E^{\infty}(R).$$

First observation: $P \longleftrightarrow X$.

$$P = (X : 1 : Z) = \big(X : 1 : \mathtt{f}(X)\big),$$

with $\mathtt{f}(x) \in \mathbb{Z}[a_1, \ldots, a_6][x]$.

3 Multiplication Polynomials

Scalar multiplication

$$nP = (\psi_1(n)X + \psi_2(n)X^2 + \ldots + \psi_{k-1}(n)X^{k-1} : 1 : \mathtt{f}(\ldots)),$$

where $k \in \mathbb{N}$ is the nilpotency of R.

Theorem

For every $i \in \{1, \ldots, k-1\}$, we have

$$\psi_i(n) \in \mathbb{Q}[a_1, \ldots, a_6][n]_i.$$

Moreover, we have $n \mid \psi_i(n)$ and

$$(2! \cdot 3! \cdot \ldots \cdot i!)\psi_i(n) \in \mathbb{Z}[a_1, \ldots, a_6][n]_i.$$

3 Super-efficient point multiplication at infinity

Over rings with nilpotency k, you only need to pre-compute

$$\psi_1(n), \psi_2(n), \ldots, \psi_{k-1}(n) \in \mathbb{Q}[a_1, \ldots, a_6][n]_{\leq k-1}.$$

Then, finding

$$nP = (\psi_1(n)X + \psi_2(n)X^2 + \ldots + \psi_{k-1}(n)X^{k-1} : 1 : \mathtt{f}(\ldots))$$

only requires (at most) k polynomial evaluations, of degree $1, 2, \ldots, k$.

Remarkable remark

It does not even directly depend on n (and the size of R)!

4 Outline

KU LEUVEN

4 Ring recap

- R finite ring of your choice, may always write $R \simeq R_1 \times ... \times R_s$ as product of finite local rings.
- We have
$$E(R) \simeq E(R_1) \times \ldots \times E(R_s).$$
- On every $E(R_i)$, we have super fast point arithmetic at infinity.
- Usually
$$E(R_i) \simeq E^{\infty}(R_i) \times E(\mathbb{F}_{q_i}).$$
- It does not look like your ECDLP benefits from working over rings!

4 Take-home message

Think carefully when choosing your favorite elliptic curve for ECDLP-based protocols.

If you run out of fantasy, have a look at https://safecurves.cr.yp.to/.
... Or propose better curves!

D. J. Bernstein, T. Lange. *SafeCurves: choosing safe curves for elliptic-curve cryptography*. https://safecurves.cr.yp.to, accessed 26 July 2023.

Thanks for your attention!