Some Open Problems Relating to the Elliptic Curve Discrete Logarithm Problem (ECDLP)

Steven Galbraith

November 1, 1999

Centre for Applied Cryptographic Research,
Faculty of Mathematics,
University of Waterloo,
Waterloo, Ontario, Canada.

Royal Holloway University of London.

sgalbrai@cacr.math.uwaterloo.ca

Elliptic curves

An **elliptic curve** is non-singular curve

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

with $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_q$.

Points are (x, y) with $x, y \in \mathbb{F}_q$ which satisfy the equation.

There is a **point at infinity** $\mathcal{O}$.

There is a process which, given two points (x_1, y_1) and (x_2, y_2), gives a third point (x_3, y_3).

Call this process **addition**.

Points on the elliptic curve are an **abelian group**.

Given $P = (x, y)$ and an integer n can efficiently compute

$$nP = \underbrace{(x, y) + (x, y) + \cdots + (x, y)}_{n \text{ times}}$$

using the **double-and-add** method.

The elliptic curve discrete logarithm problem (ECDLP)

$P = (x, y)$ a point on an elliptic curve.

Order of the point P is the smallest number $L > 0$ such that

$$LP = \mathcal{O}.$$

Assume that L is a 'large' prime.

Suppose that $Q = (x', y')$ is some other point of order L.

Then there is some number λ such that

$$Q = \lambda P.$$

The **ECDLP** is to find this number λ.

This problem is believed to be **hard**.

Elliptic curve cryptography (ECC)

$P = (x, y)$ a point of prime order L on an elliptic curve.

One-way function: Can compute $Q = nP$ efficiently. But it is computationally infeasible to obtain the number n from just the points P and Q.

Diffie-Hellman key exchange.

A		B
$S = sP$	$\longrightarrow\xrightarrow{S}\longrightarrow$	
	$\longleftarrow\xleftarrow{T}\longleftarrow$	$T = tP$
sT		tS

$$(st)P$$

Elliptic curve digital signature algorithm (ECDSA)

A has secret key d and public key $Q = dP$.

Function $f : \mathbb{F}_q \to \mathbb{Z}/L\mathbb{Z}$.

To **sign** a message $m \in \mathbb{Z}/L\mathbb{Z}$.

1. Choose random k and compute $(x_1, y_1) = kP$.

2. Put $r = f(x_1)$ and $s = k^{-1}(m+dr) \pmod{L}$

3. Send (r, s).

To **verify** signature compute

$$(x_2, y_2) = (s^{-1}m)P + (s^{-1}r)Q.$$

and test that $f(x_2) = r$.

How hard is the ECDLP?

Known methods to solve ECDLP:

Generic group methods

- Shanks' baby-step-giant-step.
- Pollard ρ and λ.
- Parallel Pollard λ.

Methods based on group homomorphism from elliptic curve $E(\mathbb{F}_q)$ to some subgroup of $\mathbb{F}_{q^k}$.

- Menezes-Okamoto-Vanstone, Frey-Rück.
- Anomalous curves. Semaev, Rück, Smart, Satoh-Araki.

Other methods?

Dimension

Dimension one

Dimension two

Dimension three

Abelian varieties

Discrete logarithm problem on an **abelian variety** is hard in general.

Important special case: Jacobian of a curve.

There are index calculus algorithms to solve the discrete logarithm problem in the Jacobian of a curve.

These algorithms are efficient when the dimension g is sufficiently large.

Possible strategy

Turn an elliptic curve discrete logarithm problem into a discrete logarithm problem on the Jacobian of a curve.

This can be done but elliptic curve discrete logarithm problem gets drowned.

Strategy: Want to reduce the size of the field as we increase the dimension.

A Cryptographic Application of Weil Descent

Steven Galbraith and Nigel Smart

October 29 1999

Centre for Applied Cryptographic Research,
Faculty of Mathematics,
University of Waterloo,
Waterloo, Ontario, Canada.

`sgalbrai@cacr.math.uwaterloo.ca`

Special acknowledgement to Gerhard Frey

1. The elliptic curve discrete logarithm problem (ECDLP)

An **elliptic curve** is non-singular curve

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

over a finite field $\mathbb{F}_q$.

Points form a finite abelian group.

ECDLP: Given $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ find $\lambda \in \mathbb{Z}$ such that $Q = \lambda P$.

ECDLP believed to be hard in general.

Discrete logarithm problem (DLP) in the Jacobian of a high-genus curve is 'easier'.

A possible attack on the ECDLP is to translate it to a DLP on the Jacobian of a curve.

2. Weil restriction of scalars

Let E be an elliptic curve over $\mathbb{F}_{q^n}$ where $n > 1$.

The **Weil restriction of scalars** of E with respect to the (Galois) extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is an abelian variety A over $\mathbb{F}_q$ of dimension n such that $A(\mathbb{F}_q) \cong E(\mathbb{F}_{q^n})$.

Example: $\mathbb{F}_{11^3} = \mathbb{F}_{11}[t]/(t^3 + t + 4)$.

$$E : y^2 = x^3 + t$$

$$(y_0 + y_1 t + y_2 t^2)^2 = (x_0 + x_1 t + x_2 t^2)^3 + t$$

Weil restriction is:

$$y_0^2 + 3y_1y_2 = x_0^3 + 7x_1^3 + 9x_0x_1x_2 + x_1x_2^2 + 5x_2^3$$
$$2y_0y_1 + 9y_1y_2 + 7y_2^2 =$$
$$3x_0^2x_1 + 10x_1^3 + 5x_0x_1x_2 + 10x_1^2x_2 + 10x_0x_2^2 + 3x_1x_2^2 + 8x_2^3 + 1$$
$$y_1^2 + 2y_0y_2 + 10y_2^2 =$$
$$3x_0x_1^2 + 3x_0^2x_2 + 8x_1^2x_2 + 8x_0x_2^2 + 10x_1x_2^2 + x_2^3$$

Points of $E(\mathbb{F}_{11^3})$ correspond to points of $A(\mathbb{F}_{11})$.

3. The idea of Weil descent

Given an elliptic curve E over $\mathbb{F}_{q^n}$ with $n > 1$:

1. Construct the Weil restriction A over $\mathbb{F}_q$. Write T_1 and T_2 for the points of the DLP on A.

2. Find a curve C over $\mathbb{F}_q$ such that there is a map $\phi : C \longrightarrow A$.

   There is a group homomorphism

   $$Jac(C)(\mathbb{F}_q) \longrightarrow A(\mathbb{F}_q).$$

3. Pull the discrete logarithm problem from $A(\mathbb{F}_q)$ back to $Jac(C)(\mathbb{F}_q)$.

4. Solve the DLP in $Jac(C)(\mathbb{F}_q)$ using an index calculus method.

4. Construction of A

$E : y^2 + xy = x^3 + b$ over $\mathbb{F}_{2^{4m}}$ with m odd.

$$\mathbb{F}_{2^4} = \mathbb{F}_2[t]/(t^4 + t + 1)$$

$$\theta = t^3 \text{ satisfies } 1 + \theta + \theta^2 + \theta^3 + \theta^4$$

Consider the basis $\{\theta, \theta^2, \theta^4, \theta^8\}$ for $\mathbb{F}_{2^{4m}}/\mathbb{F}_{2^m}$.

$$b = b_0\theta + b_1\theta^2 + b_2\theta^4 + b_3\theta^8$$

$$x = x_0\theta + x_1\theta^2 + x_2\theta^4 + x_3\theta^8$$

$$y = y_0\theta + y_1\theta^2 + y_2\theta^4 + y_3\theta^8$$

Obtain four equations in the eight variables $x_0, \ldots, x_3, y_0, \ldots, y_3$.

These equations given an affine model for a four-dimensional abelian variety over $\mathbb{F}_{2^m}$.

5. Finding the curve C

Intersect the affine variety with three hyperplanes

$$x_0 = x_1 = x_2 = x_3$$

to obtain a curve which passes through the zero point of A.

$$y_3^2 + y_0 x_0 + x_0^3 + b_0 = 0$$

$$y_0^2 + y_1 x_0 + x_0^3 + b_1 = 0$$

$$y_1^2 + y_2 x_0 + x_0^3 + b_2 = 0$$

$$y_2^2 + y_3 x_0 + x_0^3 + b_3 = 0$$

Eliminate y_1, y_2 and y_3 to get the curve C

$$y^{16} + x^{15} y =$$
$$x^{24} + x^{20} + x^{18} + x^{17} + b_0 x^{14} + b_3^2 x^{12} + b_2^4 x^8 + b_1^8.$$

6. Some comments on the curve C

The curve C is a singular curve.

There is some non-singular curve of genus g and a rational map

$$\phi : C \longrightarrow A.$$

There is some point $P_0 \in C(\mathbb{F}_q)$ which corresponds to to the zero point of A.

There is a map $C \longrightarrow Jac(C)$ given by

$$P \longmapsto (P) - (P_0).$$

The map $\phi : C \longrightarrow A$ factors as

$$C \longrightarrow Jac(C) \xrightarrow{\psi} A.$$

If A is a simple abelian variety of dimension n then the genus g of the curve C must be at least n. In this case A appears as a simple factor in the decomposition of $Jac(C)$.

7. Pulling back the DLP to Jac(C)

$Jac(C)$ can be represented as a divisor class group and the map $Jac(C) \to A$ can be given by

$$\psi : \sum_{i=1}^{d} ((Q_i) - (P_0)) \longmapsto \sum_{i=1}^{d} \phi(Q_i).$$

Want to find points $Q_i = (x_i, y_i)$ which map to a given point T on A.

The conditions

$$Q_i \text{ lie on } C, \qquad \text{and} \qquad \sum_{i=1}^{d} \phi(Q_i) = T$$

give roughly $d+n$ equations in the $2d$ variables x_i and y_i.

So, when $d > n$ we expect solutions.

8. Solving the discrete logarithm problem

Have two divisors D_1 and D_2 in $Jac(C)$ such that $D_2 \equiv \lambda D_1 (\text{mod } \ker(\psi))$.

Two strategies

- **Function field sieve**. Adleman-DeMarrais-Huang, Galbraith-Paulus-Smart.

- **Hafner-McCurley method**. Paulus, Gaudry-Morain, Hess.

When the field $\mathbb{F}_q$ is fixed and when the genus g is sufficiently large, the heuristic complexity of these algorithms is

$$\exp\left(c\sqrt{\ln q^g \ln\ln q^g}\right).$$

9. Constraints and limitations

There are two parameters

The degree of the Weil restriction n.

The genus of the curve g.

The original ECDLP is in a group of size q^n.

Some steps of the computation are difficult when n is large.

DLP algorithm in the Jacobian is efficient only when g is sufficiently large.

The complexity of the DLP algorithm is in terms of q^g, so g should not be too much larger than n.

10. Conclusion

It is possible that the Weil descent attack outlined in this talk can be used to solve certain cases of the ECDLP more efficiently than any other known method.

For elliptic curves over fields $\mathbb{F}_{2^m}$ where m is a prime, it is unlikely that the Weil descent attack we have described would give an efficient solution to the ECDLP.