MOV attack on discrete logarithm problem for elliptic curves over finite fields

Veljko Vranić

Elliptic curves and cryptography course

byblos94@gmail.com

January 27, 2024

Overview

1. Problem statement
2. Pairing intro
3. MOV Attack

Problem

The problem of finding value $k \in \mathbb{Z}$, such that $a = b^k$, for elements a, b in some group G, is called a discrete logarithm problem.

In the world of elliptic curves, we know that its points with rational coordinates form a group. In that setup, the problem is formulated as trying to find value $k \in \mathbb{Z}$ such that $P = kQ$ for P, Q points on an elliptic curve.

For practical purposes, algorithms on elliptic curves are always considered over finite fields, instead of $\mathbb{Q}$. In this specific case, the DLP problem will be considered over a finite field $\mathbb{F}_p$, where p is a prime number.

Two similar problems

DLP for $\mathbb{F}_{p^n}$
If $a, b \in \mathbb{F}_{p^n}$ and $b = a^k$
find k.

DLP for $E/\mathbb{F}_p$
If $P, Q \in E/\mathbb{F}_p$ and $Q = kP$
find k.

Two similar problems

DLP for $\mathbb{F}_{p^n}$
If $a, b \in \mathbb{F}_{p^n}$ and $b = a^k$
find k.

Computationally easy
(Index calculus)

DLP for $E/\mathbb{F}_p$
If $P, Q \in E/\mathbb{F}_p$ and $Q = kP$
find k.

Computationally hard
(Baby step, Giant step)

Weil pairing

Given elliptic curve $E/\mathbb{Q}$ and integer $m \geq 1$
$e_m : E[m] \times E[m] \mapsto$ m-th roots of unity (Weil pairing).

Such that:

- **B**illiear $e_m(P+T, Q) = e_m(P, Q)e_m(T, Q)$

Weil pairing

Given elliptic curve $E/\mathbb{Q}$ and integer $m \geq 1$
$e_m : E[m] \times E[m] \mapsto$ m-th roots of unity (Weil pairing).

Such that:

- **B**illiear $e_m(P + T, Q) = e_m(P, Q)e_m(T, Q)$
- **A**lternating $e_m(P, Q) = e_m(Q, P)^{-1}$

Weil pairing

Given elliptic curve $E/\mathbb{Q}$ and integer $m \geq 1$
$e_m : E[m] \times E[m] \mapsto$ m-th roots of unity (Weil pairing).

Such that:

- **B**illiear $e_m(P + T, Q) = e_m(P, Q)e_m(T, Q)$
- **A**lternating $e_m(P, Q) = e_m(Q, P)^{-1}$
- **N**on-degenerate $(\forall Q)e_m(P, Q) = 1 \iff P = 0$

Roots of unity and finite fields

Langrange's theorem - group theory

For any finite field $\mathbb{F}_{p^k}$, where p is prime and $k \in \mathbb{N}$,
if element $a \in \mathbb{F}_{p^k} \setminus \{0\}$, then $a^{p^k-1} = 1$.

Roots of unity and finite fields

Langrange's theorem - group theory

For any finite field $\mathbb{F}_{p^k}$, where p is prime and $k \in \mathbb{N}$,
if element $a \in \mathbb{F}_{p^k} \setminus \{0\}$, then $a^{p^k-1} = 1$.

Corollary

$(p^k - 1)st$ roots of unity is a subset of $\mathbb{F}_{p^k}$, where p is prime and $k \in \mathbb{N}$.

Roots of unity and finite fields

Langrange's theorem - group theory

For any finite field $\mathbb{F}_{p^k}$, where p is prime and $k \in \mathbb{N}$,
if element $a \in \mathbb{F}_{p^k} \setminus \{0\}$, then $a^{p^k-1} = 1$.

Corollary

$(p^k - 1)st$ roots of unity is a subset of $\mathbb{F}_{p^k}$, where p is prime and $k \in \mathbb{N}$.

Weil pairing for finite fields

Elliptic curve $E/\mathbb{F}_p$ and integer $m \geq 1$
$e_m : E[m] \times E[m] \mapsto \mathbb{F}_{p^k}$, for sufficiently large k such that $m|p^k - 1$ and **BAN** properties are satisfied.

MOV attack - idea

The MOV attack is named after Menezes, Okamoto, and Vanstone.

MOV attack - idea

The MOV attack is named after Menezes, Okamoto, and Vanstone.

DLP for $\mathbb{F}_{p^n}$		DLP for $E/\mathbb{F}_p$
If $a, b \in \mathbb{F}_{p^n}$ and $b = a^k$ find k.	Weil pairing $\Longleftarrow$	If $P, Q \in E/\mathbb{F}_p$ and $Q = kP$ find k.

MOV attack

Problem:
Elliptic curve $E/\mathbb{F}_p$, points $P, Q \in E(\mathbb{F}_p)$. Let N be the order of point P, such that $(N, p) = 1$. Find k, such that $P = kQ$.

1. Pick random point $T \in E[m]$, such that P, T generates $E[m]$

MOV attack

Problem:
Elliptic curve $E/\mathbb{F}_p$, points $P, Q \in E(\mathbb{F}_p)$. Let N be the order of point P, such that $(N, p) = 1$. Find k, such that $P = kQ$.

1. Pick random point $T \in E[m]$, such that P, T generates $E[m]$
2. Compute
$$\zeta_1 = e_N(P, T) \in \mathbb{F}_{p^m}$$
$$\zeta_2 = e_N(Q, T) \in \mathbb{F}_{p^m}$$
for m sufficiently big.

MOV attack

Problem:
Elliptic curve $E/\mathbb{F}_p$, points $P, Q \in E(\mathbb{F}_p)$. Let N be the order of point P, such that $(N, p) = 1$. Find k, such that $P = kQ$.

1. Pick random point $T \in E[m]$, such that P, T generates $E[m]$
2. Compute
$$\zeta_1 = e_N(P, T) \in \mathbb{F}_{p^m}$$
$$\zeta_2 = e_N(Q, T) \in \mathbb{F}_{p^m}$$
for m sufficiently big.
3. This reduces the problem to solving for k in $\mathbb{F}_{p^m}$

$$\zeta_2 = e_N(Q, T) = e_N(kP, T) = e_N(P, T)^k = \zeta_1^k$$

MOV attack - numeric example

Problem:
Elliptic curve $y^2 = x^3 - x$ over $E/\mathbb{F}_{29}$ and $P(17, 13)$, $Q(17, 16)$.
Find k, such that $P = kQ$. Order of P is 4.

- Checking $(N, p) = (4, 29) = 1$.

MOV attack - numeric example

Problem:
Elliptic curve $y^2 = x^3 - x$ over $E/\mathbb{F}_{29}$ and $P(17, 13)$, $Q(17, 16)$.
Find k, such that $P = kQ$. Order of P is 4.

- Checking $(N, p) = (4, 29) = 1$. ✓

MOV attack - numeric example

Problem:
Elliptic curve $y^2 = x^3 - x$ over $E/\mathbb{F}_{29}$ and $P(17, 13)$, $Q(17, 16)$.
Find k, such that $P = kQ$. Order of P is 4.

- Checking $(N, p) = (4, 29) = 1$. ✓
- Choosing a random point T from $E[N]$, such that points P and T generate $E[N]$. One such point is $T(12, 11)$.

MOV attack - numeric example

Problem:
Elliptic curve $y^2 = x^3 - x$ over $E/\mathbb{F}_{29}$ and $P(17, 13)$, $Q(17, 16)$.
Find k, such that $P = kQ$. Order of P is 4.

- Checking $(N, p) = (4, 29) = 1$. ✓
- Choosing a random point T from $E[N]$, such that points P and T generate $E[N]$. One such point is $T(12, 11)$.
- Calculating $\zeta_1 = e_4(P, T) = 28$ and $\zeta_2 = e_4(Q, T) = 28$
  Both are elements of $\mathbb{F}_{29}$

MOV attack - numeric example continued

- Solving $\zeta_2 = \zeta_1^k$ in $\mathbb{F}_{29}$

$$\frac{\zeta_1}{\zeta_2} = \frac{e_4(P, T)}{e_4(Q, T)} = e_4(P - Q, T) = e_4(P - kP, T) = e_4(P, T)^{(1-k)} = \zeta_1^k$$

$$1 = \frac{28}{28} = 28^{1-k} = -1^{(1-k)}$$

MOV attack - numeric example continued

- Solving $\zeta_2 = \zeta_1^k$ in $\mathbb{F}_{29}$

$$\frac{\zeta_1}{\zeta_2} = \frac{e_4(P,T)}{e_4(Q,T)} = e_4(P-Q,T) = e_4(P-kP,T) = e_4(P,T)^{(1-k)} = \zeta_1^k$$

$$1 = \frac{28}{28} = 28^{1-k} = -1^{(1-k)}$$

This is possible only if k is odd and since $Q = kP$ and $4P = \infty$, the only options are $k = 1$ or $k = 3$. As $P \neq Q$, we conclude that $k = 3$.

MOV attack - conclusion

Even though this attack is theoretically significant, in practice the value m could be large, in which case the discrete log problem in the group $\mathbb{F}_{p^m}^*$ is just as hard as the original discrete log problem in $E(\mathbb{F}_p)$.

MOV attack - conclusion

Even though this attack is theoretically significant, in practice the value m could be large, in which case the discrete log problem in the group $\mathbb{F}_{p^m}^*$ is just as hard as the original discrete log problem in $E(\mathbb{F}_p)$.

However, the attack forced cryptographers to pay attention while choosing elliptic curves and avoid certain types of them (supersingular elliptic curves) that are vulnerable to this attack.

The End