5.3 The MOV Attack

Rong-Jaye Chen

Department of Computer Science, National Chiao Tung University

ECC 2008

Outline

Introduction

- The MOV attack, named after Menezes, Okamoto, and Vanstone (1993), uses the Weil pairing to convert discrete log problem in $E(F_q)$ to one in $F_{q^m}^*$
- Let E be an elliptic curve over $\mathbb{F}_q$. Let $P, Q \in E(\mathbb{F}_q)$. Let N be the order of P. Assume that

$$\gcd(N, q) = 1.$$

Want to find k such that $Q = kP$.

Lemma 5.1

Lemma 5.1

$P, Q \in E(F_q),\ N = ord(P),\ \mathrm{gcd}(N, q) = 1$

$\exists\ k$ *such that* $Q = kP$ *if and only if* $NQ = \infty$ *and* $e_N(P, Q) = 1$

Proof of Lemma 5.1

Proof:

- "only if" part:

  $Q = kP \quad \rightarrow \quad NQ = kNP = \infty$

  also $e_N(P,\, Q) = e_N(P,\, P)^k = 1^k = 1$

- "if" part:

  $\gcd(N,\, q) = 1$, we have $E[N] \simeq \mathbb{Z}_N \oplus \mathbb{Z}_N$

  Choose a point R such that $\{P,\, R\}$ is a basis of $E[N]$

  Then $Q = aP + bR$

  By Corollary 3.10, $e_N(P,\, R) = \zeta$ is a primitive Nth root of unity.

  If $e_N(P,\, Q) = 1$, then $1 = e_N(P,\, Q) = e_N(P,\, P)^a\, e_N(P,\, R)^b = \zeta^b$

  $\rightarrow \; b \equiv 0 \pmod{N}$

  $\rightarrow \; bR = \infty$

  $\rightarrow \; Q = aP$

MOV attack - (1)

- Choose m , such that $E[N] \subset E(F_{q^m})$
  By Corollary 3.11, $\mu_N \subset F_{q^m}$
- MOV attack (Want to solve $Q = kP$ for k.)
  1. Choose a random point $T \in E(F_{q^m})$
  2. Compute $M = ord(T)$
  3. Let $d = \text{gcd}(M, N)$, and let $T_1 = (M/d)T$
     Then $d = ord(T_1)$, $d \mid N$, so $T_1 \in E[N]$
  4. Compute $\zeta_1 = e_N(P, T_1)$ and $\zeta_2 = e_N(Q, T_1)$
     Then both $\zeta_1, \zeta_2 \in \mu_d \subseteq F^*_{q^m}$
  5. Solve discrete logarithm problem

     $$\zeta_2 = \zeta_1^k \quad \text{in } F^*_{q^m}$$

     This will give k (mod d)
  6. Repeat with random points T until the lcm of d's is N .
     This determines k (mod N)

MOV attack - (2)

- Potentially, m could be large, in which case the discrete log problem in group $F_{q^m}^*$ is just as hard as the original discrete log problem in $E(F_q)$. However, for supersingular curves, we can usually take $m = 2$.

Proposition 5.3

Proposition 5.3

E/F_q, suppose $a = q + 1 - \#E(F_q) = 0$
If $\exists\ P \in E(F_q)$ of order N, then $E[N] \subset E(F_{q^2})$

Proof:

(1) $\phi_q^2 - a\phi_q + q = 0$
$\rightarrow\ \phi_q^2 = -q \quad (\because a = 0)$

(2) Let $S \in E[N]$
$\because ord(P) = N\ ,\ \#E(F_q) = q + 1$
$\rightarrow\ N \mid q + 1 \quad \Leftrightarrow \quad -q \equiv 1 \pmod{N}$
By (1),
$\phi_q^2(S) = -qS = 1 \cdot S = S$
By Lemma 4.5, $S \in E(F_{q^2})$