# ELLIPTIC CURVES CRYPTOGRAPHY

FRANCESCO PAPPALARDI

## #3 - ELLIPTIC CURVES ATTACKS.

SEPTEMBER $16^{\text{TH}}$ 2015

**National University of Mongolia**
Ulan Baatar, Mongolia
September 16, 2015

# Weil Pairing



Let $E/K$ and $m \in \mathbb{N}$ s.t. $p \nmid m$. Then

$$E[m] \cong C_m \oplus C_m$$

We set

$$\mu_m := \{x \in \bar{K} : x^m = 1\}$$

$\mu_m$ is a cyclic group with $m$ elements(since $p \nmid m$)

**Theorem (Existence of Weil Pairing)**

*There exists a pairing $e_m : E[m] \times E[m] \to \mu_m$ called Weil Pairing, s.t. $\forall P, Q \in E[m]$*

1. $e_m(P +_E Q, R) = e_m(P, R)e_m(Q, R)$ *(bilinearity)*
2. $e_m(P, R) = 1 \forall R \in E[m] \Rightarrow P = \infty$ *(non degeneracy)*
3. $e_m(P, P) = 1$
4. $e_m(P, Q) = e_m(Q, P)^{-1}$
5. $e_m(\sigma P, \sigma Q) = \sigma e_m(P, Q) \ \forall \sigma \in \mathrm{Gal}(\bar{K}/K)$
6. $e_m(\alpha(P), \alpha(Q)) = e_m(P, Q)^{\deg \alpha} \ \forall \alpha$ *separable endomorphism*

The last one needs to be discussed further!!!

# Properties of Weil pairing





$E[m] \cong C_m \oplus C_m \;\Rightarrow\; E[m]$ has a $\mathbb{Z}/m\mathbb{Z}$*–basis*

i.e.

$$\exists P, Q \in E[m] : \forall R \in E[m], \exists! \alpha, \beta \in \mathbb{Z}/m\mathbb{Z}, R = \alpha P + \beta Q$$

**Proposition**

If $(P, Q)$ is a $\mathbb{Z}/m\mathbb{Z}$–basis, then $\zeta = e_m(P, Q) \in \mu_m$ is *primitive* (i.e. $\operatorname{ord} \zeta = m$)

**Proof.**

Let $d = \operatorname{ord} \zeta$. Then

$$1 = e_m(P, Q)^d = e_m(P, dQ).$$

$\forall R \in E[m]$ write $R = \alpha P + \beta Q$. Hence

$$e_m(R, dQ) = e_m(P, dQ)^\alpha e_m(Q, Q)^{d\beta} = 1$$

So $dQ = \infty \;\Rightarrow\; m \mid d$. $\square$

## Properties of Weil pairing (continues)

**Proposition**

$$E[m] \subset E(K) \Rightarrow \mu_m \subset K$$

**Proof.**

Let $\sigma \in \mathrm{Gal}(\bar{K}/K)$. Since the basis $(P, Q) \subset E(K)$,

$$\sigma(P) = P, \sigma(Q) = Q.$$

Hence

$$\zeta = e_m(P, Q) = e_m(\sigma P, \sigma Q) = \sigma e_m(P, Q) = \sigma\zeta$$

So

$$\zeta \in \bar{K}^{\mathrm{Gal}(\bar{K}/K)} = K \Rightarrow \mu_n = \langle\zeta\rangle \subset K^*$$

□

**Corollary**

$$E(\mathbb{F}_q) \cong C_n \oplus C_{kn} \Rightarrow q \equiv 1 \bmod n$$

**Proof.**

$$E[n] \subset E(\mathbb{F}_q) \Rightarrow \mu_n \subset \mathbb{F}_q^* \Rightarrow n \mid q - 1$$

□

If $E/\mathbb{Q} \Rightarrow E[m] \not\subseteq E(\mathbb{Q})$ for $m \geq 3$

## The MOV attack



First proposed by: MENEZES, ALFRED J.; OKAMATO, TATSUAKI; VANSTONE, SCOTT A. (1993). "*Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field*". IEEE Transactions On Information Theory **39** (5).

It allows to reduce the comutation of a DL in $E(\mathbb{F}_q)$ to a DL in $\mathbb{F}_{q^m}$ (for a suitable $m \in \mathbb{N}$).

- Hence if $m < 5$, there is a problem!
- we observed that DL in finite fields may be five times more unsafe then DL in elliptic curves
- We shall discuss the case of supersingular curves where $m = 2$
- Hence, supersingular curves are NOT idoneous for ECC.
- We assume that $E/\mathbb{F}_q$ is an elliptic curve
- We shall also assume that the Weil pairing can be computed quickly (which is not obvious)

## The MOV attack

- Assume that $P, Q \in E(\mathbb{F}_q)$ and that $N = \text{ord}\, P$
- Also assume that $\gcd(q, N) = 1$ so that $E[N] \cong \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$.
- We want to find $k$ such that

$$Q = kP$$

- Such a $k$ may not exist!! However

**Proposition**

There exists $k$ such that $Q = kP$ if and only if

- $NQ = \infty$
- $e_N(P, Q) = 1$

**Proof.**

(if): if $NQ = \infty$, then $Q \in E[N]$. We choose $R \in E[N]$ in such a way that $\{R, P\}$ is basis for $E[N]$.
Then

$$Q = aP + bR, \exists a, b \in \mathbb{Z}/N\mathbb{Z}$$

From basic properties of Weil pairing, $e_N(P, R) = \zeta$ is a primitive $N$–th root of unity.Hence, if $e_N(P, Q) = 1$,

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

We deduce that $b \equiv 0 \bmod N$. So $bR = \infty$ and $Q = aP$ as requested.
(only if): just note that $NQ = NkP = \infty$ and $e_N(P, Q) = e_N(P, P)^k = 1$. □

# The MOV attack

## the idea

Given $E$, $P$, $Q$ and $N = \text{ord}\, Q$, choose $m$ s.t. $E[N] \subset E(\mathbb{F}_{q^m})$.

Note that

- such an $m$ exists since $E[N] \subset E(\overline{\mathbb{F}_q})$. So it is enough to choose $m$ such that $\mathbb{F}_{q^m}$ contains all coordinates of all point in $E[N]$.
- Since $\deg \phi_N = (N^2 - 1)/2$, we can find a suitable $m < ((N^2 - 1)/2)!$
- We shall do all our computation in $\mathbb{F}_{q^m}$

**ALGORITHM:**

1. Choose at random $T \in E(\mathbb{F}_{q^m})$
2. Compute the order $M$ of $T$
3. Let $d = \gcd(M, N)$, and let $T' = \frac{M}{d}T$. $T'$ has order $d$ which is a divisor of $N$. Hence $T' \in E[N]$
4. Compute $\zeta_1 = e_N(P, T')$ and $\zeta_2 = e_N(Q, T_1)$. Then $\zeta_1, \zeta_2 \in \mu_d \subset \mathbb{F}_{q^m}^*$
5. Solve DL $\zeta_2 = \zeta_1^k \in \mathbb{F}_{q^m}^*$. This will give $k \bmod d$.
6. Repeat with random points untill the lcm of the $d'$s obtained in $N$. This determines $k$ modulo $N$.

# The MOV attack

**why does it work?**

## ALGORITHM:

1. Choose at random $T \in E(\mathbb{F}_{q^m})$
2. Compute the order $M$ of $T$
3. Let $d = \gcd(M, N)$, and let $T' = \frac{M}{d}T$. $T'$ has order $d$ which is a divisor of $N$. Hence $T' \in E[N]$
4. Compute $\zeta_1 = e_N(P, T')$ and $\zeta_2 = e_N(Q, T_1)$. Then $\zeta_1, \zeta_2 \in \mu_d \subset \mathbb{F}_{q^m}^*$
5. Solve DL $\zeta_2 = \zeta_1^k \in \mathbb{F}_{q^m}^*$. This will give $k \bmod d$.
6. Repeat with random points untill the lcm of the $d'$s obtained in $N$. This determines $k$ modulo $N$.

Let $k_d := k \bmod d$ and note

$$\zeta_2 = e_N(Q, T_1) = e_N(kP, T_1) = \zeta_1^k = \zeta_1^{k_d}$$

since $\zeta_1$ and $\zeta_2$ have both order $d$

If we compute $k_{d_1}, \cdots, k_{d_s}$ with the property that

$$\text{lcm}(d_1, \cdots, d_s) = N.$$

Then, by the General Chinese remainder Theorem, we can compute $k \bmod N$ which is the DL!

Once can verify that the probability that $d = 1$ is quite small.

# The MOV attack

## Supersingular curves are unsuitable for EEC

**Definition**

An elliptic curve is called supersingular if, when we write

$$E(\mathbb{F}_q) = q + 1 - a_E,$$

we have

$$a_E \equiv 0 \bmod p.$$

**Theorem**

*Suppose $E/\mathbb{F}_q$ is supersingular and that $a_E = 0$. If $P \in E(\mathbb{F}_q)$ and $N = \text{ord}\, P$. Then*

$$E[N] \subset E(\mathbb{F}_{q^2})$$

- We shall prove the theorem now
- For other types of supersingular curves (i.e. with $a_E \equiv 0 \bmod p$ but $a_E \neq 0$, it can be proven that If $P \in E(\mathbb{F}_q)$ and $N = \text{ord}\, P$. Then

$$E[N] \subset E(\mathbb{F}_{q^m}) \qquad \text{with } m = 3, 4, 6.$$

- Supersingular curves are not suitable for EEC

## The Frobenius endomorphism $\Phi_q$

$$\Phi_q : \bar{\mathbb{F}}_q \to \bar{\mathbb{F}}_q, x \mapsto x^q \text{ is a field automorphism}$$

Given $\alpha \in \bar{\mathbb{F}}_q$,

$$\alpha \in \mathbb{F}_{q^n} \Leftrightarrow \Phi_q^n(\alpha) = \alpha^{q^n} = \alpha$$

Fixed points of powers of $\Phi_q$ are exactly elements of $\mathbb{F}_{q^n}$

$$\Phi_q : E(\bar{\mathbb{F}}_q) \to E(\bar{\mathbb{F}}_q), (x, y) \mapsto (x^q, y^q), \infty \mapsto \infty$$

**Properties of $\Phi_q$**

- $\Phi_q(x, y) = (x, y) \iff (x, y) \in E(\mathbb{F}_q)$
- $\Phi_q^n(x, y) = (x^{q^n}, y^{q^n})$ so $\Phi_q^n(x, y) = (x, y) \Leftrightarrow (x, y) \in \mathbb{F}_{q^n}$
- $\Phi_q$ satisfies the Carachteristic polynomial $T^2 - a_E T + q$
  i.e.
  $$\forall (x, y) \in E(\overline{F_q}), (x^{q^2}, y^{q^2}) +_E q(x, y) = a_E(x^q, y^q)$$
- we write the above identity as
  $$\Phi_q^2 - a_E \Phi_q + q = 0.$$

# The MOV attack

## Supersingular curves are unsuitable for EEC

**Theorem**

*Suppose $E/\mathbb{F}_q$ is supersingular and that $a_E = 0$. If $P \in E(\mathbb{F}_q)$ and $N = \operatorname{ord} P$. Then*

$$E[N] \subset E(\mathbb{F}_{q^2})$$

**Proof.**

Since $a_E = 0$, the Frobenius $\Phi_q$ satisfies

$$\Phi_q^2 = -q$$

Suppose that $P \in E(\mathbb{F}_q)$ has order $N$. Then $N \mid q + 1$ (i.e. $q \equiv -1 \mod N$).
Let $S \in E[N]$, Then

$$\Phi_{q^2}(S) = \Phi_q^2(S) = -qS = S.$$

This implies that $S \in E(\mathbb{F}_{q^2})$. □

## Anomalous Curves

**Definition**

An elliptic curve is called anomalous if, when we write

$$\#E(\mathbb{F}_q) = q$$

- In an anomalous curve points have order equal to a power of $p$. Hence the Weil pairing is not defined!!!
- One may think that they are suitable for Cryptography for this reason. But this is not true!!
- There is an efficient algorithm to compute DL in anomalous curves
- If $E$ is anomalous, then $a_E = -1$
- The carachteristic polynomial of $E$ is $T^2 - T + q$ with roots:

$$\frac{1+\sqrt{1-4q}}{2} \quad \frac{1-\sqrt{1-4q}}{2}$$

- Hence
$$\#E(\mathbb{F}_{q^n}) = q^2 + 1 - \tfrac{1}{2^n}\left((1+\sqrt{1-4q})^n + (1-\sqrt{1-4q})^n\right)$$
- So $\#E(\mathbb{F}_{q^2}) = q^2 + 2q$ and $E/\mathbb{F}_{q^2}$
- An anamalous curve is not necessarily anomalous over field extensions but it still satisfies $\Phi_q^2 - \Phi_q + q = 0$.

## Anomalous Curves

**Definition**

An elliptic curve is called anomalous if, when we write

$$\#E(\mathbb{F}_q) = q$$

- Examples:
  1. $E' : y^2 + xy = x^3 + x^2 + 1$ is anomalous over $\mathbb{F}_2$
  2. $E'' : y^2 = x^3 + x^2 - 1$ is anomalous over $\mathbb{F}_3$
- They are particularly suitable for Cryptography when considered over extensions
  1. They group order can be computed very quickly
     - $\#E'(\mathbb{F}_{2^{200}}) = 2^{200} + 1 - \frac{(1+\sqrt{-7})^{200}+(1-\sqrt{-7})^{00}}{2^{100}} = 1606938044258990275541962092343697546215565682541130425732128$
     - $\#E''(\mathbb{F}_{3^{150}}) = 3^{200} + 1 - \frac{(1+\sqrt{-11})^{150}+(1-\sqrt{-11})^{150}}{2^{150}} =$ $369988485035126972924700782451696645401107717195926015868067750551938000$
  2. Computations are fast on them
- From $\Phi_q^2 - \Phi_q + q = 0$ we deduce
- $\forall P = (x, y) \in E(\mathbb{F}_{q^n})$

$$q(x, y) = (x^q, y^q) + (x^{q^2}, -y^{q^2})$$

- Instead of computing $qP$ one can just compute $x^q, y^q, x^{q^2}, y^{q^2}$ which is fast in a finite field
- Especially if one uses normal basis

## Normal basis on $\mathbb{F}_q$

**Definition**

Let $\mathbb{F}_{q^m}$ be a finite field extension of $\mathbb{F}_q$ and let $\beta \in \mathbb{F}_{q^m}^*$. We say that $\beta$ is normal if

$$\mathcal{B}_\beta = \{\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^{m-1}}\}$$

is an $\mathbb{F}_q$–basis of $\mathbb{F}_{q^m}$.

- $\mathcal{B}_\beta$ is called normal basis
- It is a classical result that every finite field admits a normal basis.
- Given an $\mathbb{F}_q$–normal basis of $\mathbb{F}_{q^m}$ and given $x \in \mathbb{F}_{q^m}^*$, we write

$$x = x_0\beta + x_1\beta^q + \cdots + x_{m-2}\beta^{q^{m-1}}$$

- So

$$x^p = x_0\beta^q + x_1\beta^{q^2} + \cdots + x_{m-2}\beta$$

- Since $\beta^{q^m} = \beta$
- There is no calculation in computing $x^q$ but just a circular rotation of the coefficients
- Going back to anomalous curves:

$$q(x, y) = (x^q, y^q) + (x^{q^2}, -y^{q^2})$$

- implies that $q(x, y)$ can be computed in an anomalous curve at the cost of one addition in $E$

# Further Reading...


Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart, Advances in elliptic curve cryptography, London Mathematical Society Lecture Note Series, vol. 317, Cambridge University Press, Cambridge, 2005.

J. W. S. Cassels, Lectures on elliptic curves, London Mathematical Society Student Texts, vol. 24, Cambridge University Press, Cambridge, 1991.

John E. Cremona, Algorithms for modular elliptic curves, 2nd ed., Cambridge University Press, Cambridge, 1997.

Anthony W. Knapp, Elliptic curves, Mathematical Notes, vol. 40, Princeton University Press, Princeton, NJ, 1992.

Neal Koblitz, Introduction to elliptic curves and modular forms, Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1984.

Joseph H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.

Joseph H. Silverman and John Tate, Rational points on elliptic curves, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.

Lawrence C. Washington, Elliptic curves: Number theory and cryptography, 2nd ED. Discrete Mathematics and Its Applications, Chapman & Hall/CRC, 2008.

Horst G. Zimmer, Computational aspects of the theory of elliptic curves, Number theory and applications (Banff, AB, 1988) NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., vol. 265, Kluwer Acad. Publ., Dordrecht, 1989, pp. 279–324.