III. The Tate-Lichtenbaum Pairings: Miller's loop and some improvements

B. Adrian Dina

Reilabs:

Cryptography Seminar

03 July 2024

The Tate-Lichtenbaum Pairings (TLP's)

Remember: There are two problems when considering the TLP,

$$\langle \cdot, \cdot \rangle_n : E(K)[n] \times E(K)/nE(K) \to K^*/(K^*)^n$$
$$(P, Q) \mapsto \langle P, Q \rangle_n = f_P(D_Q),$$

namely:

- It takes values in the quotient $K^*/(K^*)^n$, and
- for a given $P \in E(K)[n]$, there is a rational function $f_P \in K^*(E)$ whose divisor is

$$[f_P] = n[P] - n[\mathcal{O}_E].$$

  How to compute $f_P(D_Q)$ computationally effective?
- Keep in mind: In practice n will be very big, i.e. $n \geq 2^{160}$ and since $\deg(f_P) \approx n$, it's impossible to compute these functions without some more "sophisticated" approach.

The Tate-Lichtenbaum Pairings (TLP's)

Now:

- In order to solve the first issue, we proved that raising any representative $\langle P, Q \rangle_n$ in $K^*/(K^*)^n$ to the power $(q^k - 1)/n$ result in a unique element in group of the nth. roots of unity μ_n; in other words

$$K^*/(K^*)^n \xrightarrow{\sim} \mu_n,$$
$$\langle P, Q \rangle_n \mapsto \langle P, Q \rangle_n^{(q^k-1)/n}$$

  is an isomorphism of groups. We call this step the final exponentiation.

- This step ensures that different parties can compute the exact same value under the bilinearity property, rather than values which are the same under equivalence.

The Tate-Lichtenbaum Pairings (TLP's)

- Unfortunately, the final exponentiation is very expensive since $q^k - 1$ is for cryptographic cases very large; more precisely, Cohen-Frey: Handbook of E&HCC suggest that

$$\#\mathbb{F}_{q^k} \geq 2^{1024} - \text{elements, where } K = \mathbb{F}_{q^k}.$$

- We will discuss in this talk techniques how the final exponentiation step can be handled more efficiently.

The Tate-Lichtenbaum Pairings (TLP's)

- The other part of our discussion today will handle the question: for given $P \in E(K)[n]$ find the rational function $f_P \in K^*(E)$ with
$$[f_P] = n[P] - n[\mathcal{O}_E]$$
such that for any representative $Q \in K^*/(K^*)^n$ with divisor
$$D_Q \sim [Q] - [\mathcal{O}_E], \text{ and } \sup(D_Q) \cap \sup([f_P]) = \{\},$$
and compute $f_P(D_Q)$ effectively.
- An effective solution for this problem is called the Miller loop; Victor Miller described an algorithm to compute the Weil pairing in polynomial time which can be also used in the case of the Tate-Lichtenbaum pairing.

Today's roadmap

- Computing the Tate pairing via Miller's loop.
- Some general improvements.
- A last observation.

The Tate-Lichtenbaum Pairings: The Setup

Setup: Let $K_0 = \mathbb{F}_q$ be a finite field of characteristic p. Further, let

- $(E, \mathcal{O}_E)$ be an elliptic curve defined over K_0;
- n be a positive integer coprime to p which divides $\#E(K_0)$;
- k be the embedding degree of n and
- K be the extension $K_0(\mu_n) \cong \mathbb{F}_{q^k}$, where $\mu_n := \mu_n(K_0)$.

Consider the following groups:

- $E(K)[n] = \{P \in E(K) : [n]P = \mathcal{O}_E\}$,
- $nE(K) = \{[n]P : P \in E(K)\}$,
- $E(K)/nE(K) = \{P + nE(K) : P \in E(K)\}/\sim$,
  where
  $P + nE(K) \sim Q + nE(K)$, if and only if $P + (-Q) \in nE(K)$.

Intermezzo: Is the Tate-Lichtenbaum pairing well defined

Martin's question: Is the Tate-Lichtenbaum pairing

$$\begin{aligned} \langle\cdot,\cdot\rangle_n : E(K)[n] \times E(K)/nE(K) &\to K^*/(K^*)^n \\ (P,Q) &\mapsto \langle P,Q\rangle_n = f_P(D_Q), \end{aligned}$$

well defined as an element of $K^*/(K^*)^n$.

Intermezzo: Is the Tate-Lichtenbaum pairing well defined

Claim: Let $P \in E(K)[n]$ and let $f \in K(E)$, such that

$$[f] = n[P] - n[\mathcal{O}_E].$$

Let D_1, D_2 be divisors on E defined over K with disjoint support from $\{\mathcal{O}_E, P\}$.

- Suppose $D_1 \sim D_2 \sim [Q] - [\mathcal{O}_E]$ for some $Q \in E(K)$. Then

$$f(D_1)/f(D_2) \in (K^*)^n.$$

- Suppose $D_1 \sim [Q_1] - [\mathcal{O}_E]$ and $D_2 \sim [Q_2] - [\mathcal{O}_E]$ for some $Q_1, Q_2 \in E(K)$ and $Q_1 \neq Q_2$ and $Q_1 - Q_2 \in nE(K)$. Then

$$f(D_1)/f(D_2) \in (K^*)^n.$$

Intermezzo: Is the Tate-Lichtenbaum pairing well defined

Proof of part one:

- Write $D_2 = D_1 + \mathrm{div}(h)$ with $h \in K(E)$ and where $\sup(h) \cap \{\mathcal{O}_E, P\} = \{\}$. Then

$$f(D_2) = f(D_1 + \mathrm{div}(h)) = f(D_1) \cdot f(\mathrm{div}(h)).$$

We apply Weil-Reciprocity (WR), and get that

$$\begin{aligned} f(\mathrm{div}(h)) =_{WR} h(\mathrm{div}(f)) &= h(n[P] - n[\mathcal{O}_E]) \\ &= (h(P)/h(\mathcal{O}_E))^n \in (K^*)^n. \end{aligned}$$

Intermezzo: Is the Tate-Lichtenbaum pairing well defined

Proof of part two:

- Write $Q_1 - Q_2 = nQ'$ for some $Q' \in E(K)$, $Q' \neq \mathcal{O}_E$. Then

$$[Q_1] - [Q_2] = n(\ [Q' + S] - [S]\ ) + \mathrm{div}(h_0)$$

for some $h_0 \in K(E)$ and $S \in E(\bar{K})$ with

$$S \notin \{\mathcal{O}_E, -Q', P, P - Q'\}.$$

Further we have

$$\begin{aligned} D_1 &= [Q_1] - [\mathcal{O}_E] + \mathrm{div}(h_1) \\ D_2 &= [Q_2] - [\mathcal{O}_E] + \mathrm{div}(h_2) \end{aligned}$$

for some $h_i \in K(E)$.

$$\begin{aligned} f(D_2) &= f\left(D_1 - n(\ [Q' + S] - [S]\ ) + \mathrm{div}(h_2) - \mathrm{div}(h_1) - \mathrm{div}(h_0)\right) \\ &= f(D_1) \cdot f([Q' + S] - [S])^n \cdot f(\mathrm{div}(h_2/h_0 h_1)). \end{aligned}$$

Intermezzo: Is the Tate-Lichtenbaum pairing well defined

Exercise. Show that if

$$\mathrm{sup}(\mathrm{div}(h_2/h_0h_1)) \subseteq M := \bigcup_{i=1}^{2} \mathrm{sup}(D_i) \cup \{Q' + S, S\}, \text{ and}$$
$$M \cap \{\mathcal{O}_E, P\} = \{\}, \text{ then}$$

apply Weil-Reciprocity and show that $f(\mathrm{div}(h_2/h_0h_1)) \in (K^*)^n$. Then $f(D_1)/f(D_2) \in (K^*)^n$.

Remark: For a proof of Weil-Reciprocity for algebraic curves, see e.g. Blake-Seroussi-Smart: Advances in Elliptic Curve Cryptography.

The Miller Function

Remember: For a given $P \in E(K)[n]$, how do we find the rational function $f_{n,P} \in K^*(E)$, such that

$$[f_{n,P}] = n[P] - n[\mathcal{O}_E].$$

Definition: Let $P \in E(K)$ and let m be a positive integer. A Miller function is a function $f_{m,P} \in K(E)$, such that

$$\mathrm{div}(f_{m,P}) = m[P] - [mP] - (m-1)[\mathcal{O}_E].$$

Remark: For all $m \in \mathbb{Z}$ and $P \in E$, we have that

- $f_{m,P} \in \mathrm{Div}^0(E)$ since $\deg(f_{m,P}) = 0, m - 1 - (m-1) = 0$, and $sum(f_{m,P}) = mP - mP = \mathcal{O}_E$.
- Further, if $P \in E[m]$, then $f_{m,P} = m[P] - m[\mathcal{O}_E]$, and
- We can evaluate $f_{m,P}(Q)$ at any $Q \neq P, \mathcal{O}_E$.

The Miller Function

Proposition: Show that $f_{1,P} = 1$ and if $f_m = f_{m,P}, f_s = f_{s,P}$ are Miller functions, then

$$f_{m+s} = f_m \ f_s \ \frac{\ell_{mP,sP}}{v_{(m+s)P}},$$

where $\ell_{mP,sP}, v_{(m+s)P} \in \bar{K}[x, y]$ are lines arising in the elliptic curve addition of

$$mP + sP = (m+s)P.$$

Proof: First we notice, that $\mathrm{div}(f_1) = [P] - [P] - 0[\mathcal{O}_E] = [0]$ is the zero devisor and one can take $f_1 := 1$ to be constant. Then write

$$\begin{aligned}
\mathrm{div}(\ell_{mP,sP}) &= [mP] + [sP] + [-(m+s)P] - 3[\mathcal{O}_E], \\
\mathrm{div}(v_{(m+s)P}) &= [(m+s)P] + [-(m+s)P] - 2[\mathcal{O}_E], \text{ and} \\
\mathrm{div}(\ell_{mP,sP}/v_{(m+s)P}) &= [mP] + [sP] - [(m+s)P] - [\mathcal{O}_E],
\end{aligned}$$

The Miller Function

and so:

$$\begin{aligned}\operatorname{div}\left(f_m f_s \frac{\ell_{mP,sP}}{v_{(m+s)P}}\right) &= m[P]-[mP]-(m-1)[\mathcal{O}_E]+\\ &\quad m[P]-[mP]-(m-1)[\mathcal{O}_E]+\\ &\quad [sP]+[sP]-[(m+s)P]-[\mathcal{O}_E]\\ &= m[P]+s[P]-[(m+s)P]+(m+s-1)[\mathcal{O}_E]\\ &= (m+s)[P]-[(m+s)P]+(m+s-1)[\mathcal{O}_E]\\ &= \operatorname{div}(f_{m+s}).\end{aligned}$$

Corollary: Using the additive identity of $f_{m,P}$, we have that

$$f_{2m,P} = f_{m,P}^2 \, \frac{\ell_{mP,mP}}{v_{(2m)P}}.$$

Computing the Tate Pairing via Miller's loop

Remarks: We have seen above that the divisor

$$\mathrm{div}(f_{m,P}) = m[P] - [mP] - (m-1)[\mathcal{O}_E]$$

can be updated to the divisor

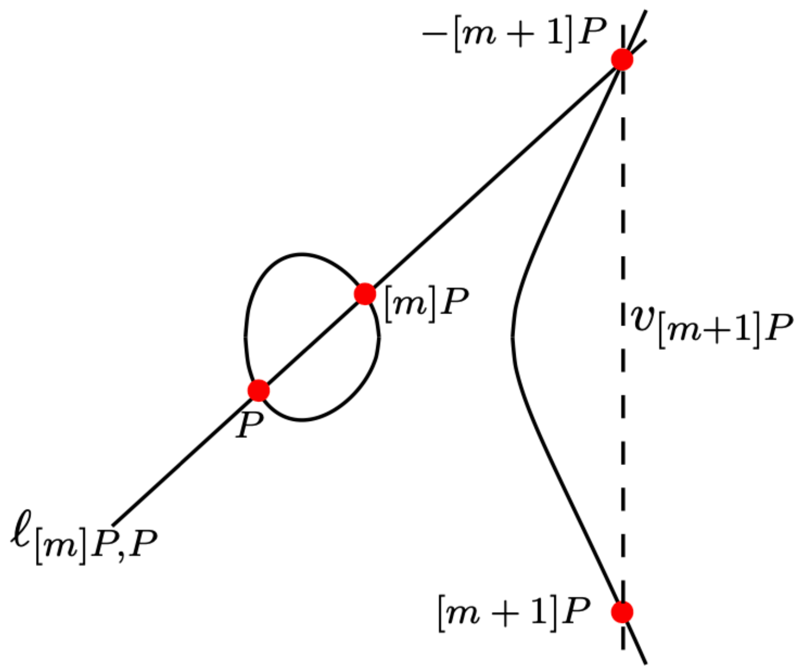
$$\mathrm{div}(f_{m+1,P}) = (m+1)[P] - [(m+1)P] - m[\mathcal{O}_E]$$

by adding the divisor

$$\mathrm{div}(\ell_{mP,P}/v_{(m+1)P}) = [P] + [mP] - [(m+1)P] - [\mathcal{O}_E],$$

which corresponds to the multiplication of functions

$$f_{m+1} = f_m \frac{\ell_{mP,P}}{v_{(m+1)P}}.$$



$-[m+1]P$
$[m]P$
P
$v_{[m+1]P}$
$\ell_{[m]P,P}$
$[m+1]P$

Miller's Algorithm

We can now give Miller's algorithm to compute $f_{n,P}(D_Q)$ for any divisor D_Q over K, such that

$$D_Q \sim [Q] - [\mathcal{O}_E]$$

for $Q \in E(K)/nE(K)$, and where in many cases for applications

$$D_Q = [Q+S] - [S] \text{ for } S \in E(K).$$

Basic Idea:

- Use a "square-and-multiply" strategy in order to compute the Miller function out of smaller Miller functions.

Remember, that for given Miller functions

$$f_{m,P} = m[P] - [mP] - (m-1)[P],$$
$$f_{m+1,P} = (m+1)[P] - [(m+1)P] - m[P],$$

we can use the additive identity of the Miller function and write

Miller's Algorithm

$$f_{m+1,P} = f_{m,P} \cdot \frac{\ell_{mP,P}}{v_{(m+1)P}},$$

with divisor

$$\operatorname{div}\left(\frac{\ell_{mP,P}}{v_{(m+1)P}}\right) = [P] + [mP] - [(m+1)P] - [\mathcal{O}_E].$$

Basic Idea:

- Start with $\operatorname{div}(f_{2,P}) = 2[P] - [2P] - [\mathcal{O}_E]$ and repeat the construction from above $(n-1)$-times in order to get the Miller desired function

$$f_{n,P} = n[P] - [nP] - (n-1)[\mathcal{O}_E] = n[P] - n[\mathcal{O}_E].$$

- Consider the last step in the computation of $f_{n,P}$,

$$\begin{aligned} f_{n-1,P} &= (n-1)[P] - [(n-1)P] - (n-2)[\mathcal{O}_E] \\ &= f_{n-2,P} \cdot \frac{\ell_{(n-2)P,P}}{v_{(n-1)P}}, \text{ with} \end{aligned}$$

Miller's Algorithm

$$\mathrm{div}\left(\frac{\ell_{(n-2)P,P}}{v_{(n-1)P}}\right) = [P] + [(n-1)P] - 2[\mathcal{O}_E],$$

and which because of the relation $(n-1)P = -P$ for $P \in E[n]$,

$$[P] + [(n-1)P] - 2[\mathcal{O}_E] = \mathrm{div}(v_P) = \mathrm{div}(v_{-P}) = \mathrm{div}(v_{(n-1)P}).$$

Then, the pairing evaluating function $f_{n,P}$ is the product

$$f_{n,P} = (\ell_{(n-2)P,P}) \cdot \prod_{i=1}^{n-3} \frac{\ell_{iP,P}}{v_{(i+1)P}},$$

and where $v_P = v_{1.P}$ is not part of the product, since $f_1 = 1$.

Miller's Algorithm

Remark: Let's write down the contribution for an quotient $\frac{\ell_{iP,P}}{v_{(i+1)P}}$ and consider the sum of their divisors:

$$
\begin{aligned}
\ell_{P,P}/v_{(2)P} &: P + P - 2P - \mathcal{O}_E \\
\ell_{P,P}/v_{(2)P} &: P + 2P - 3P - \mathcal{O}_E \\
\ell_{P,P}/v_{(2)P} &: P + 3P - 4P - \mathcal{O}_E \\
&\vdots \\
\ell_{(n-3)P,P}/v_{(n-2)P} &: P + (n-3)P - (n-2)P - \mathcal{O}_E \\
\ell_{(n-2)P,P} &: P + (n-2)P + (-(n-1)P) - 3\mathcal{O}_E.
\end{aligned}
$$

Miller's Algorithm

Then $\mathrm{div}(\ell_{(n-2)P,P}) + \sum \mathrm{div}(\ell_{iP,P}/v_{(i+1)P}) = \ldots =$ is given by

$$(n-1)[P] + [-(n-1)P] - n[\mathcal{O}_E] = n[P] - n[\mathcal{O}_E],$$

since $(n-1)P = -P$.

Remarks:

- By construction $f_{n,P} = g(x,y)/h(x,y)$ is a rational function on E and where $\deg(g) = \deg(h) = n$.
- The explained method computes $f_{n,P}$ successively by increasing the degree of g and h in each step; when n is exponentially large, the method hat exponential complexity.

Miller's Algorithm

Miller's Observation: Consider the following divisors,

- $[f_{m,P}] = m[P] - [mP] - (m-1)[\mathcal{O}_E]$,
- $[f_{m,P}^2] = 2m[P] - 2[mP] - 2(m-1)[\mathcal{O}_E]$,
- $[f_{2m,P}] = 2m[P] - [(2m)P] - (2m-1)[\mathcal{O}_E]$.

Then $[f_{2m,P}] - [f_{m,P}^2] = 2[mP] - [(2m)P] - [\mathcal{O}_E] \in \mathrm{Div}^0(E)$, which is given by a rational function with

- a <u>zero of order two at mP</u>, and
- <u>simple poles at $(2m)P$ and $\mathcal{O}_E$</u>.

But this is exactly the additive identity in our previous corollary,

$$f_{2m,P} = f_{m,P}^2 \, \frac{\ell_{mP,mP}}{v_{(2m)P}}.$$

Miller's Algorithm

Putting everything together we see, that

- Getting form $f_{m,P}$ to $f_{m+1,P}$, $f_{2m,P}$ fast, Miller observed that this procedure gives rise to a double-and-add style algorithm; to get to $f_{2m,P}$ requires logarithmic-time-steps.
- Since $f_{m,P}$ becomes too large to store, Miller's next idea is to evaluate at every stage s, $f_{s,P}(D_Q)$; in other words, instead of storing at any stage s an element $f_{s,P} \in \mathbb{F}_{q^k}(E)$, store the value $f_{s,P}(D_Q) \in \mu_n \subset \mathbb{F}_{q^k}$. This step requires the final exponentiation.

Miller's Algorithm

Input: $P \in E(K)[n]$, $D_Q \sim [Q] - [\mathcal{O}_E]$, $n = (n_{m-1} \ldots n_1 n_0)_2$ with $n_{m-1} = 1$.
Output: $f_{n,P}(D_Q)$.

$R \leftarrow P$, $f \leftarrow 1$.
for $i = (m-2)$ to 0 **do**
    Compute line functions $\ell_{R,R}$, v_{2R} for doubling R.
    $R \leftarrow 2R$.
    $f \leftarrow f^2 \cdot \frac{\ell_{R,R}}{v_{2R}}(D_Q)$.
    if $m_i = 1$ **then**
        Compute line functions $\ell_{R,P}$, v_{R+P} for adding R and P.
        $R \leftarrow R + P$.
        $f \leftarrow f^2 \cdot \frac{\ell_{R,P}}{v_{R+P}}(D_Q)$.
    end if
end for
return f.

An Explicit Example

Example[1]: Let $E/\mathbb{F}_p : y^2 = x^3 + 21x + 15$, where $p = 47$ and where $\#E(\mathbb{F}_p) = 51$.

Consider the following setup: Take $n = 17$ and

- compute the embedding degree $k = k_n$ with respect to n. i.e. the minimal k, such that $n|(p^k - 1)$, which is 4.
- Let $K := \mathbb{F}_{p^4} = \mathbb{F}_p(\zeta)$, where ζ is a root of the polynomial $x^4 - 4x^2 + 5 \in \mathbb{F}_p[x]$.
- Let $P, Q \in E(K)$ with

$$P = (45, 23),\ \ Q = (31\zeta^2 + 29, 35\zeta^3 + 11\zeta),$$

and check that $P \in E(\mathbb{F}_p)[n]$ and $Q \in E(K)[n]\backslash E(\mathbb{F}_p)[n]$.

[1]See C. Costello; Pairings for beginners, page 79.

An Explicit Example

Task: Use Miller's algorithm and compute

$$\langle P, Q \rangle_n = f_{n,P}(D_Q)^{(q^k-1)/n}.$$

Do:

- Write $n = 17 = (1,0,0,0,1)_2$ and take
- Take $D_Q = [2Q] - [Q]$ and see that $D_Q \sim [Q] - [\mathcal{O}_E]$, since

$$D_Q - [Q] + [\mathcal{O}_E] = 2[Q] - [2Q] - (2-1)[\mathcal{O}_E]$$

  represents $\operatorname{div}(f_{2,Q})$.

Question: Why is $\sup(D_Q) \cap \sup(f_{n,P}) = \{\}$?

An Explicit Example

We consider each steps in Miller's algorithm:

- Step 1: Set $R := P = (45, 23)$ and $f = 1$.
- Step 2: $(i, r_i) = (3, 0)$:
  - Step 3: Compute $\ell_{R,R} = y + 33x + 43$, $v_{(2)R} = x + 35$.
  - Step 4: Set $R := 2R = (12, 16)$.
  - Step 5: Set $f(D_Q) := f^2 \cdot \frac{\ell_{R,R}}{v_{(2)R}}(D_Q) = 41\zeta^3 + 32\zeta^2 + 2\zeta + 21$.
- Step 2: $(i, r_i) = (2, 0)$:
  - Step 3: Compute $\ell_{R,R} = y + 2x + 7$, $v_{(2)R} = x + 20$.
  - Step 4: Set $R := 2R = (27, 14)$.
  - Step 5: Set $f(D_Q) := f^2 \cdot \frac{\ell_{R,R}}{v_{(2)R}}(D_Q) = 22\zeta^3 + 27\zeta^2 + 30\zeta + 33$.

An Explicit Example

We consider each steps in Miller's algorithm:

- Step 2: $(i, r_i) = (1, 0)$:
  - Step 3: Compute $\ell_{R,R} = y + 42x + 27$, $v_{(2)R} = x + 29$.
  - Step 4: Set $R := 2R = (18, 31)$.
  - Step 5: Set $f(D_Q) := f^2 \cdot \frac{\ell_{R,R}}{v_{(2)R}}(D_Q) = 36\zeta^3 + 2\zeta^2 + 21\zeta + 37$.
- Step 2: $(i, r_i) = (0, 1)$:
  - Step 3: Compute $\ell_{R,R} = y + 9x + 42$, $v_{(2)R} = x + 2$.
  - Step 4: Set $R := 2R = (45, 24)$.
  - Step 5: Set $f(D_Q) := f^2 \cdot \frac{\ell_{R,R}}{v_{(2)R}}(D_Q) = 10\zeta^3 + 21\zeta^2 + 40\zeta + 25$.
  - Step 7: Compute the final addition via line $v_{R+P} = x + 2$.
  - Step 8: Set $R := R + P = \mathcal{O}_E$ and update
  - Step 9: $f(D_Q) := 17\zeta^3 + 6\zeta^2 + 10\zeta + 22$.
- Step 12: Return $f_{n,P}(D_Q) := 17\zeta^3 + 6\zeta^2 + 10\zeta + 22$.

Then,

$$\begin{aligned}\langle P, Q\rangle_n = f_{n,P}(D_Q)^{(q^k-1)/n} &= (17\zeta^3 + 6\zeta^2 + 10\zeta + 22)^{287040} \\ &= 33\zeta^3 + 43\zeta^2 + 45\zeta + 39.\end{aligned}$$

Some general improvements.

The Initial Problem

Remeber: Let $K = \mathbb{F}_{q^k}$.

- Raising any representative $\langle P, Q \rangle_n$ in $K^*/(K^*)^n$ to the power $(q^k - 1)/n$ result in a unique element in group $\mu_n \subset K^*$. This step is called the final exponentiation.
- Unfortunately, the final exponentiation is very expensive since $q^k - 1$ is for cryptographic cases very large, $\#\mathbb{F}_{q^k} \geq 2^{1024}$.

Question: Can we express the final exponentiation with some less expensive computations?

General Improvements

Before digging explicitly into the final exponentiation, let's collect some further acceleration steps for the computation of the TLP.[2] We discuss each of these steps in the following:

- Why can we replace the divisor D_Q by the explicit point Q?
- Why can we replace $(q^k - 1)/n$ by $c \cdot (q - 1)$ for some positive integers c?
- How to construct efficiently tower field extensions.
- The final exponentiation.

[2] For a detailed discussion, see Barreto, Kim, Lynn, and Scott (BKLS) in Efficient algorithms for pairing-based cryptosystems.

General Improvements

Setup: Let $K_0 = \mathbb{F}_q$ be a finite field of characteristic p and let

- $(E, \mathcal{O}_E)$ be an elliptic curve defined over K_0;
- n, a positive integer coprime to p with $n | \#E(K_0)$;
- k, the embedding degree of n, and
- $K = K_0(\mu_n) \cong \mathbb{F}_{q^k}$, where $\mu_n := \mu_n(K_0)$.

Improvement 1: Replace the divisor D_Q by the point Q.

Theorem (Thm 1, BKLS)

With the same setup as above,

$$f_{n,P}(D_Q)^{(q^k-1)/n} = f_{n,P}(Q)^{(q^k-1)/n}$$

for any $Q \neq \mathcal{O}_E$.

General Improvements

Consequences: The theorem above "saves" us from

- defining a divisor equivalent to $D_Q = [Q] - [\mathcal{O}_E]$ with support disjoint from $[f_{n,P}]$.
- Further, it allows us to evaluate the intermediate Miller function at the single point Q rather than two points in each iteration of the algorithm.

General Improvements

Improvement 2: Replace $(q^k - 1)/n$ by $c \cdot (q - 1)$ for some positive integers c.

Lemma (Lemma 1, BKLS)

The value $q - 1$ is a factor of $(q^k - 1)/n$ for any factor n of $\#E(\mathbb{F}_q)$, where E is one of the following elliptic curves

$$E_{1,b} : y^2 = x^3 + (1 - b)x + b \textit{ with } b \in \{0, 1\},$$
$$E_{2,b} : y^2 + y = x^3 + x + b \textit{ with } b \in \{0, 1\},$$
$$E_{3,b} : y^2 = x^3 - x + b \textit{ with } b \in \{\pm 1\}.$$

General Improvements

Proof:

- Firstly, we have the following equivalence

$$\mathbb{F}_q^* \subseteq \mathbb{F}_{q^k}^* \iff \#\mathbb{F}_q^* | \#\mathbb{F}_{q^k}^* \iff (q-1)|(q^k-1).$$

- Secondly, one can show that

  $\#E_{1,b} = q+1, \ \#E_{2,b} = q+1 \pm \sqrt{2q}, \ \#E_{3,b} = q+1 \pm \sqrt{3q},$

  and where in all these cases

$$\gcd(\#E_{a,b}(\mathbb{F}_q), q-1) = 1,$$

  and since $n|\#E(\mathbb{F}_q)$ as we assumed, it follows also that

$$\gcd(n, q-1) = 1.$$

- By the two points above, we see that $(q-1)|((q^k-1)/n)$.

General Improvements

Consequences:

- Improvement 2 (and 1) allow us to write the final exponentiation as

$$f_{n,P}(Q)^{(q^k-1)/n} = \left(f_{n,P}(Q)^{(q-1)}\right)^c,$$

  with the consequence, that any $f_{n,P}(Q) \in \mathbb{F}_q$ will become to $1 = f_{n,P}(Q)^{(q-1)} \Longrightarrow 1 = \left(f_{n,P}(Q)^{(q-1)}\right)^c$ under the final exp.
- Therefore if $f_{n,P}(Q) \in \mathbb{F}_q$, we can do any operation involving $f_{n,P}(Q)$ without effecting the value of the pairing.

General Improvements

Improvement 3: How to construct efficiently tower field extensions?

More precisely: Starting from $\mathbb{F}_q$, how to construct efficiently the full extension $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$?

- For small k, choose irreducible polynomial $f(x) \in \mathbb{F}_q[x]$ of degree k. Then $\mathbb{F}_{q^k} := \mathbb{F}_q[x]/(f)$ is the desired field extension.
- For large values of k, use Koblitz-Menezes's approach.

Koblitz-Menezes's approach: Use embedding degrees of the form

$$k = 2^u 3^v$$

and construct $\mathbb{F}_{q^k}$ using a tower field of quadratic and cubic extensions.

General Improvements

Let E be an elliptic curve defined over $\mathbb{F}_p$ with embedding degree k.

Definition: We say that $\mathbb{F}_{p^k}$ is pairing-friendly if $p \equiv 1 \pmod{12}$ and $k = 2^u 3^v$.

Theorem

Let $\mathbb{F}_{p^k}$ be a pairing-friendly field, and let α be an element of $\mathbb{F}_p$ that is neither a square or a cube in $\mathbb{F}_p$. Then the polynomial $x^k - \alpha$ is irreducible in $\mathbb{F}_p[x]$.

General Improvements

Example:

- Then, by Koblitz-Menezes, $\mathbb{F}_{q^k} = \mathbb{F}_q[x]/(x^{12} - \alpha)$.
- Or choose a tower fields construction,

$$\mathbb{F}_q \xrightarrow{2\,=\,[\mathbb{F}_{q^2}:\mathbb{F}_q]} \mathbb{F}_{q^2} \xrightarrow{3\,=\,[\mathbb{F}_{q^6}:\mathbb{F}_{q^2}]} \mathbb{F}_{q^6} \xrightarrow{2\,=\,[\mathbb{F}_{q^{12}}:\mathbb{F}_{q^6}]} \mathbb{F}_{q^{12}},$$

  where

  - $\mathbb{F}_{q^2} = \mathbb{F}_q[\beta]/(\beta^2 - \alpha)$,
  - $\mathbb{F}_{q^6} = \mathbb{F}_{q^2}[\gamma]/(\gamma^3 - \beta)$,
  - $\mathbb{F}_{q^{12}} = \mathbb{F}_{q^6}[\delta]/(\delta^2 - \gamma)$.

Take (some) relative bases:

- $\mathbb{F}_{q^{12}} = \langle 1, \delta : \delta^2 = \gamma \rangle_{\mathbb{F}_{q^6}}$,
- $\mathbb{F}_{q^6} = \langle 1, \gamma, \gamma^2 : \gamma^3 = \beta \rangle_{\mathbb{F}_{q^2}}$,
- $\mathbb{F}_{q^2} = \langle 1, \beta : \beta^2 = \alpha \rangle_{\mathbb{F}_q}$.

General Improvements

Take arbitrary $a, b \in \mathbb{F}_{q^{12}}$ and write them relative, i.e.

- $a = a_0 + a_1\delta$, $b = b_0 + b_1\delta$ with $a_i, b_i \in \mathbb{F}_{q^6}$, and compute

  $$a \cdot b = (a_0 + a_1\delta)(b_0 + b_1\delta) = a_0 b_0 + (a_0 b_1 + a_1 b_0)\delta + a_1 b_1 \gamma,$$

  where each components are in in $\mathbb{F}_{q^6}$.
- Then write
  $$\begin{aligned} a_0 &= a_{0,0} + a_{0,1}\gamma + a_{0,2}\gamma^2, \\ b_0 &= b_{0,0} + b_{0,1}\gamma + b_{0,2}\gamma^2, \\ a_0 b_0 &= a_{0,0} b_{0,0} + (a_{0,0} b_{0,1} + a_{0,1} b_{0,0})\gamma + \\ &\quad (a_{0,0} b_{0,2} + a_{0,1} b_{0,1} + a_{0,2} b_{0,0})\gamma^2 + \\ &\quad (a_{0,1} b_{0,2} + a_{0,2} b_{0,1})\beta \ + \ a_{0,2} b_{0,2}\beta\gamma \end{aligned}$$

  with $a_{0,j}, b_{0,j} \in \mathbb{F}_{q^2}$. In this way the operations "move down" to $\mathbb{F}_q$.

General Improvements

Remarks:

- Because of degree reasons, a naive multiplication of two numbers in $\mathbb{F}_{q^{12}}$ over $\mathbb{F}_q$ requires $12^2 = 144$ $\mathbb{F}_q$-multiplications.
- Using the descent-method above, the naive method costs
  - 4-multiplications in $\mathbb{F}_{q^6}$, where each of these
  - requires 9-multiplications in $\mathbb{F}_{q^2}$, and where each of these requires 4-multiplications in $\mathbb{F}_q$,

  where in total $4 \cdot 9 \cdot 4 = 144$.

But: Fortunately there are faster methods in the literature which using the tower field construction allow faster operations as operations applied in the maximal extension.

The Final Exponentiation

Improvement 5: How to perform the final exponentiation efficiently?

- Assume k is <u>even</u>: Split the final exponent into three components,

$$(q^k - 1)/n = \frac{(q^d - 1) \cdot (q^d + 1)}{\Phi_k(q)} \cdot \frac{\Phi_k(q)}{n},$$

where $d = k/2$ and where $\Phi_k(\cdot)$ is Euler's totient function.

Remarks: For any $\alpha \in \mathbb{F}_{q^k}$, raising α to a power of q involves

- an action of the qth power Frobenius map.
- Further, if $\alpha \in \mathbb{F}_{q^k}$ is the value to be exponentiated, then

$$u := \alpha^{(q^d - 1)} \text{ is of relative norm } N_{\mathbb{F}_{q^k}|\mathbb{F}_{q^d}}(u) = u \cdot \bar{u} = 1$$

and inversion corresponds to conjugation.

The Final Exponentiation

Example: Consider $k = 24$ and $\Phi_{24}(x) = x^8 - x^4 + 1$. Then split

$$(q^{24} - 1)/n = ((q^{12} - 1) \cdot (q^4 + 1)) \cdot \frac{q^8 - q^4 + 1}{n}.$$

Use the expression to compute

$$f^{(q^{24}-1)/n} = \left(f^{(q^{12}-1)\cdot(q^4+1)}\right)^{(q^8-q^4+1)/n}.$$

Remarks:

- The easy part: The computations $f^{q^{12}}$, f^{q^4} are 12,4-times repeated application of the Frobenius Frob_q and it some multiplications and an inversion.
- The hard part: We remain with the exponent $q^8 - q^4 + 1/n$; then $u := \alpha^{q^{12}-1} \in \mathbb{F}_{q^{24}}$ is a unit in $\mathbb{F}_{q^{24}}$ and inversion is simple conjugation.

The Final Exponentiation

The hard part:

- One can use some further techniques in [3], and write the hard past, as some polynomials

$$\frac{q(x)^8 - q(x)^4 + 1}{n(x)} = \sum_{i-0}^{7} \lambda_i(x) q^i(x),$$

  where the polynomials $\lambda_i(x)$ depend on the underlying family of elliptic curves and have some "nice representations".
- The exact description of the $\lambda_i(x)'s$ for families of elliptic curves for cryptographic cases is discussed in SBCPK; On the final exponentiation for calculating pairings on ordinary elliptic curves.

[3] see e.g. C. Costello; On the final exponentiation for calculating pairings on ordinary elliptic curves, page 114-115.

A last observation

A last observation

Goal: Determine whether the outcome of two pairings are equal; not inside the quotient $K^*/(K^*)^n$ but equal as elements in μ_n.

Explicitly: Check wheter $\langle P, Q\rangle_n^{(q^k-1)/n} = \langle P', Q'\rangle_n^{(q^k-1)/n}$, which is equivalent to whether

$$f_{n,P}(D_Q)^{(q^k-1)/n} = f_{n,P'}(D_{Q'})^{(q^k-1)/n},$$

one can test

$$\left(\frac{f_{n,P}(D_Q)}{f_{n,P'}(D_{Q'})}\right)^{(q^k-1)/n} = 1,$$

which after improvements 1 and 2 can be written as

$$\left(\left(\frac{f_{n,P}(Q)}{f_{n,P'}(Q')}\right)^{(q-1)}\right)^c = 1.$$

A last Question

An observation:

- Assume $x := f_{n,P}(Q)$ and $y := f_{n,P'}(Q')$ are both in $\mathbb{F}_q$ and $y \neq x$, then

$$\frac{x}{y} \neq 1 \text{ but } \left(\frac{x}{y}\right)^{q-1} = 1, \text{ in } \mathbb{F}_q.$$

In other words, we cannot use this approach in general in order to check weather $\langle P, Q\rangle_n^{(q^k-1)/n} = \langle P', Q'\rangle_n^{(q^k-1)/n}$.

Thank you for listening!