Pairing : an arithmetical point of view

Nadia EL MRABET

Université Montpellier II

Journées arithmétiques Edinburgh
July 2007

Data

- $n \in \mathbb{N}^*$.
- G_1 and G_2 two additives abelian groups of order n.
- G_3 cyclic group of order n.

Definition

A pairing is a map :

$$e : G_1 \times G_2 \longrightarrow G_3$$

- *Bilinear :* $\forall P, P' \in G_1, \forall Q \in G_2$

$$e(P + P', Q) = e(P, Q).e(P', Q)$$

$$e(P, iQ) = e(P, Q)^i$$

- *Non-degenerate :*

$$\forall P \in G_1 - \{0\},\ \exists Q \in G_2\ s.t.\ e(P, Q) \neq 1$$

Destructive :

- MOV attack : Menezes, Okamoto and Vanstone.(1993)

Constructive (since 2000) :

- Tri partite Diffie Hellman key exchange.
- Identity based scheme.
- Short signature.

Weil Pairing

A natural tool

- Let E an elliptic curve over a finite field K.
- n an integer prime to $Char(K)$.
- $\overline{E[n]} = \{Q \in E(\overline{K}),\ [n]Q = P_\infty\}$.
- F_P the rationnal function such that $div(F_P) = nD_P$

For P and Q sucht that $supp(Div(F_P)) \bigcap supp(Div(F_Q)) = \emptyset$:

$$e_W : E[n] \times \overline{E[n]} \mapsto U_n$$

$$e_W(P, Q) = \frac{F_P(D_Q)}{F_Q(D_P)}$$

- E an elliptic curve over a finite field $\mathbb{F}_q$.
- $P \in E(\mathbb{F}_q)$, n the order of $< P >$.
- k the smallest integer such that $n \mid (q^k - 1)$.
- $Q \in E(\mathbb{F}_{q^k})$.
- F_P the function such that :
  $div(F_P) = n(P) - (nP) - (n-1)P_\infty$.

Weil pairing :

$$e_W(P,Q) = \frac{F_P(Q)}{F_Q(P)} \in \mathbb{F}^*_{q^k}.$$

Tate pairing :

$$e_T(P,Q) = F_P(Q)^{\frac{q^k-1}{n}} \in \mathbb{F}^*_{q^k}.$$

Which is the best ?

Miller algorithm

Calculate $F_P(Q)$

- Initialisation : $T \leftarrow P$

1. For each bit of n :
   - $T \leftarrow [2]T$
   - $$\frac{f_1}{f_2} \longleftarrow \frac{{f_1}^2}{{f_2}^2} \times \frac{h_1(Q)}{h_2(Q)}$$
2. If $n_i = 1$
   - $T \leftarrow T \oplus P$
   - $$\frac{f_1}{f_2} \longleftarrow \frac{f_1}{f_2} \times \frac{h_1(Q)}{h_2(Q)}$$

The Miller step need computation in the field extension $\mathbb{F}_{q^k}$.

Problem : computation in $\mathbb{F}_{q^k}$ are more expensive then computation in $\mathbb{F}_q$.

There is (at least) two solutions :

- Improve the arithmetic in the extension field.
  $\Rightarrow$ pairing friendly field and cyclotomic sub group.
- As soon as possible, try to calculate in the small field.
  $\Rightarrow$ representation of Q and final exponentiation for Tate.

Definition

$\mathbb{F}_{q^k}$ is a pairing friendly field if $p \equiv 1 \; mod(12)$ & $k = 2^i.3^j$.

Theorem

$\mathbb{F}_{p^k}$ a pairing friendly field, β neither a square or a cube in $\mathbb{F}_p$
Then $X^k - \beta$ irreducible over $\mathbb{F}_p$.

Consequences

$\mathbb{F}_{p^k}$ can be constructed as a tower of quadratic and cubic extensions.

$\Rightarrow$ a perceptible reduction of the cost of a multiplication in $\mathbb{F}_{p^k}$.

Improving the arithmetic (for Tate & Weil)

Cyclotomic sub group

Definition

A subgroup of $\mathbb{F}_{p^k}^*$ of order $\Phi_k(q)$

Lemma

for $k = 6$, $p \equiv 2$ *or* 5 *mod*(9)
$\mathbb{F}_{q^6}$ is defined by $g(X) = X^6 + X^3 + 1$

Consequences

- $\Rightarrow$ inversion faster because $\Phi_k(p) | (p^{k/2} + 1)$ and $\alpha^{-1} = \alpha^{p^{k/2}}$.
- $\Rightarrow$ more efficient squaring : Lenstra & Stam method.

Improving Miller operation (for Tate & Weil)

When the denominator disappears

When k is even, a better way to represent Q :

- $Q \in E(F_{q^k})$ is written $(x, y\sqrt{\beta})$
  where x, y, $\beta \in F_{q^{k/2}}$, $\sqrt{\beta} \in F_{q^k}$
- Consequence : $h_2 \in F_{q^{k/2}}$.
- Then the Miller step is : $f_1 \leftarrow {f_1}^2.h_1(Q)$.
  - For Tate because of the final exponentiation.
  - For Weil because an exponentiation does not change the result.

Improving the final exponentiation(for Tate)

To improve the computation of $\omega^{\frac{q^k-1}{n}}$:

- As $n/\Phi_k(q)$
  - $\omega^{\frac{q^k-1}{n}} = \left(\omega^{\frac{q^k-1}{\Phi_k(q)}}\right)^{\frac{\Phi_k(q)}{n}}$
- The exponentiation to the power $\frac{q^k-1}{\Phi_k(q)}$ is made in the tower of extension, so does not cost a lot.
- The more expensive operation is the power $\frac{\Phi_k(q)}{n}$.

  $\Rightarrow$ Instead of calculation in $\mathbb{F}_{q^k}$, Lucas Sequence uses elements in $\mathbb{F}_{q^{k/2}}$.

Tate or Weil in odd characteristic

k	Pairing friendly	Cyclotomic
2	Tate better for l.s. $<$ 192 bits	Nothing
6	Tate better for l.s. $<$ 256	Tate better for l.s. $<$ 256
12	Tate better for l.s. $<$ 256	Tate better for l.s. $<$ 192
24	Tate better for l.s. $<$ 256	Tate better for l.s. $<$ 256

Characteristic 2

The equations are more simple.

- Only one inversion.
- Affine coordinates more efficient then Jacobien.
- Several improvement of the Tate pairing, none for Weil.

So, Tate is more efficient than Weil.

Further work :

- Trying to improve Weil.
- Finding for which level security Weil becomes more efficient than Tate.

Thank you for your attention.