Pairing in cryptography : an arithmetic point of view

J.C. Bajard and N. El Mrabet

ARITH-LIRMM, CNRS,
Université Montpellier II, France

SPIE
August 2007

Pairings

Definition

Data

- $n \in \mathbb{N}^*$ (generally a prime number).
- G_1 and G_2 two additive abelean groups of order n.
- G_3 cyclic group of order n.

Definition

A pairing is a map :

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

which verifies the following properties :

Pairings

Definition's Properties

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

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

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

$$e(iP, Q) = e(P, Q)^i \text{ and } e(P, iQ) = e(P, Q)^i$$

- *Non-degenerate :*

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

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

Pairings

Cryptographic use

Destructive :

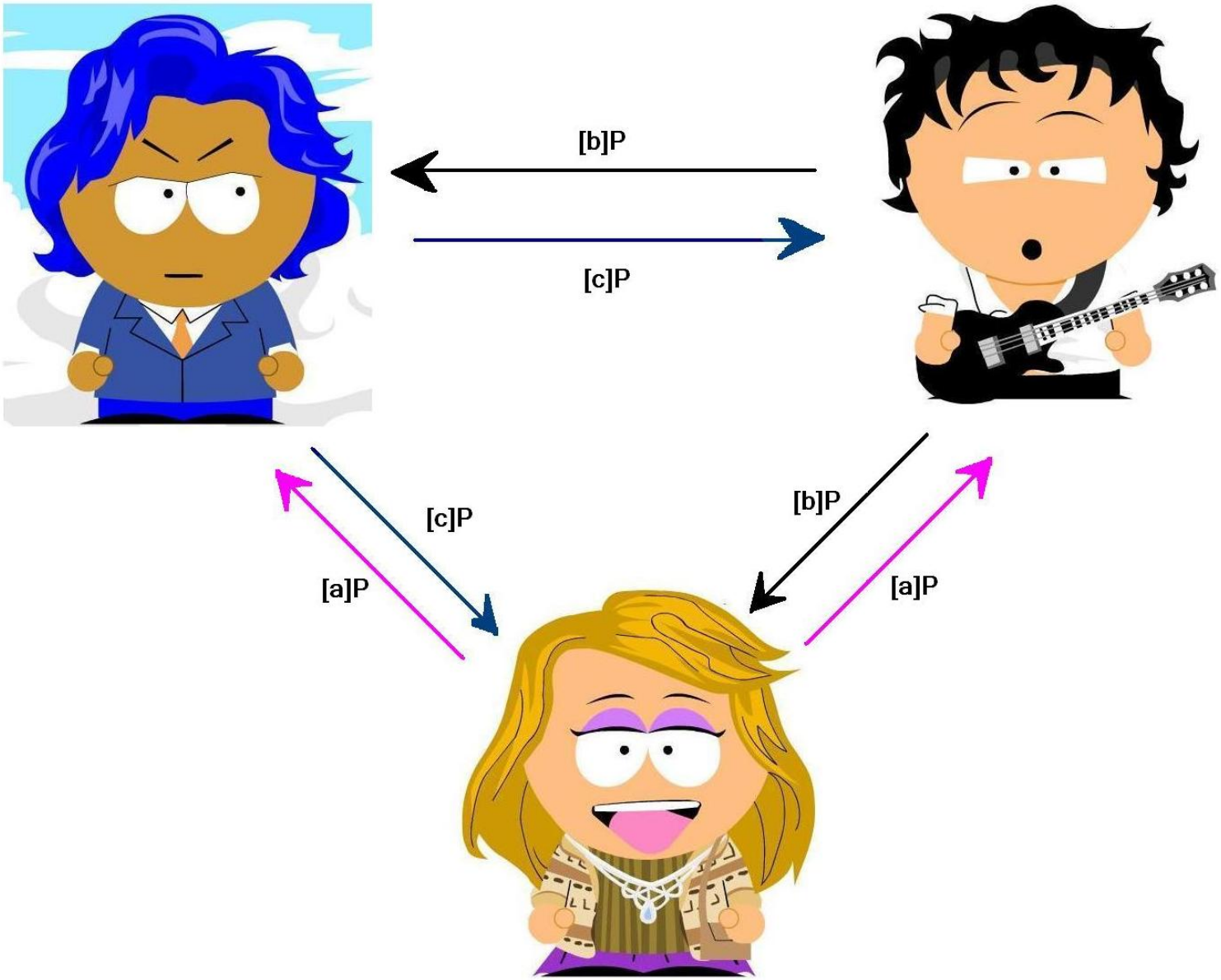
- MOV attack : Menezes, Okamoto and Vanstone (1993).

Constructive (since 2000) :

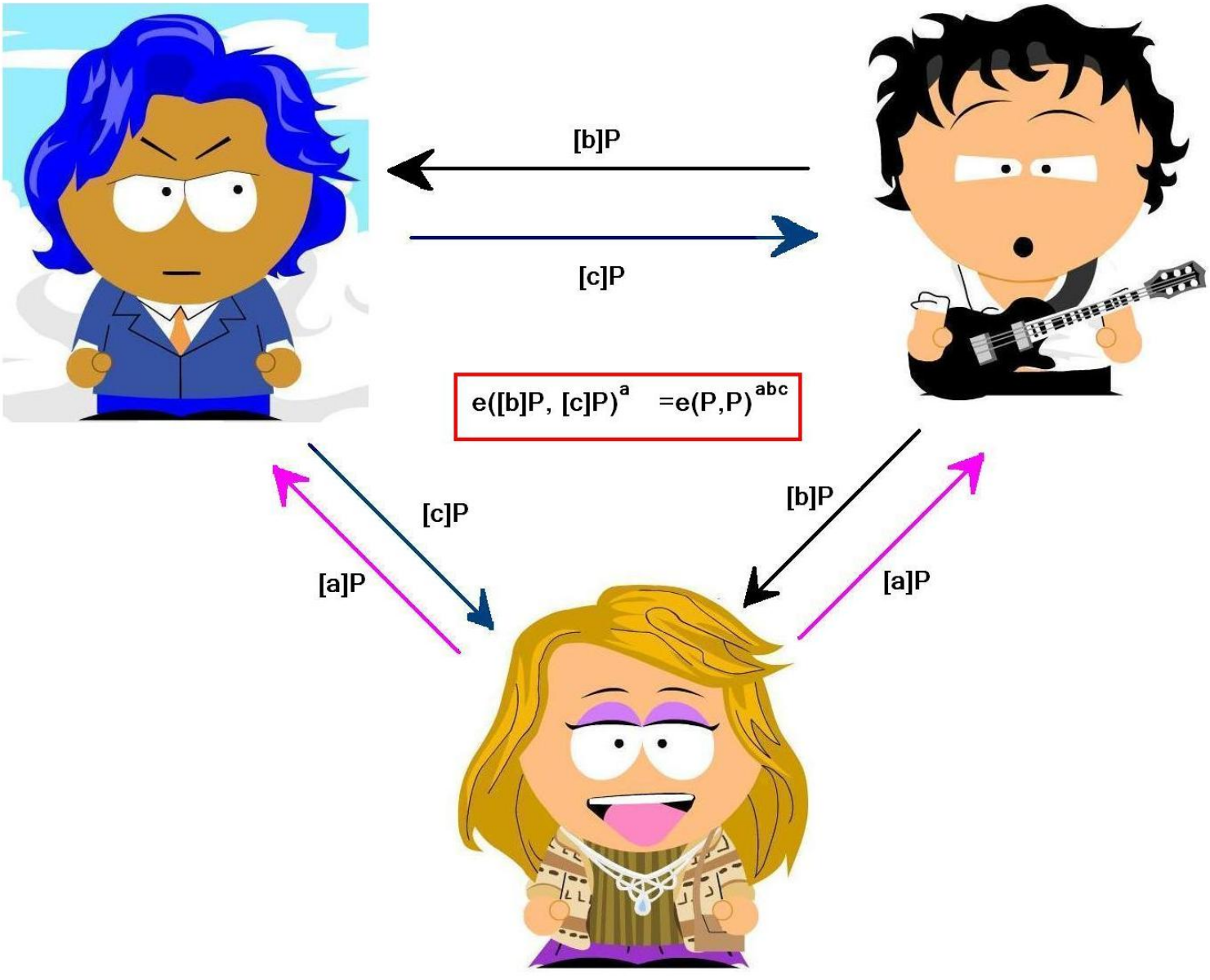
- Tri partite Diffie Hellman key exchange (by A.Joux 2000).
- Short signature (by D.Boneh, B.Lynn, H.Shacham 2001).
- Identity based scheme (by D.Boneh and M.Franklin 2003).

Tri-partite Diffie Hellman

Tri-partite Diffie Hellman



Tri-partite Diffie Hellman



Elliptic curve cryptography

Notations

- E an elliptic curve over a finite field $\mathbb{F}_p$,
- $P \in E(\mathbb{F}_p)$, n the order of $< P >$,
- $G_1 = \langle P \rangle$,
- k the smallest integer such that $n \mid (p^k - 1)$ (even in general),
- $Q \in E(\mathbb{F}_{p^k})$,
- $G_2 = \langle Q \rangle$,
- G_3 sub-group of order n of $\mathbb{F}^*_{p^k}$.

Weil versus Tate

Definitions of Weil and Tate pairings

Let $P \in E(\mathbb{F}_p)$, $Q \in E(\mathbb{F}_{p^k})$.

Weil pairing :

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

Tate pairing :

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

Weil versus Tate

Two contradictory conclusions

Two way to compute the pairing : which one is the best ?

- N.Koblitz , A.J.Menezes : ***Pairing-based cryptography at high security levels***, 2005.

  $\Rightarrow$ Weil more efficient than Tate for high level security.

- R.Granger , D.Page , N.Smart : ***High security pairing-based cryptography revisited***, 2006.

  $\Rightarrow$ Tate always more efficient than Weil.

Miller algorithm

Calculate $F_P(Q)$

- Initialisation : $T \leftarrow P$, $f_1 \leftarrow 1$ and $f_2 \leftarrow 1$.

1. For each bit of n :
   - $T \leftarrow [2]T$ (computation in $\mathbb{F}_p$)
   - $\frac{f_1}{f_2} \longleftarrow \frac{{f_1}^2}{{f_2}^2} \times \frac{h_1(Q)}{h_2(Q)}$ (computation in F_{p^k})

2. If $n_i = 1$
   - $T \leftarrow T \oplus P$ (computation in $\mathbb{F}_p$)
   - $\frac{f_1}{f_2} \longleftarrow \frac{f_1}{f_2} \times \frac{h_1(Q)}{h_2(Q)}$ (computation in F_{p^k})

Miller algorithm

How improve it ?

The Miller step need computation in the field extension $\mathbb{F}_{p^k}$, inversion, and exponentiation.

There is some solutions :

- twisted curve for evaluation in $\mathbb{F}_{p^{k/2}}$,
- elimination of the denominator evaluation,
- pairing friendly field and cyclotomic sub group,
- some improvements of the exponentiation.

Twisted curve

Definition

Let E en elliptic curve over a field $\mathbb{K}$.
$\widetilde{E}$ over $\widetilde{\mathbb{K}}$ is a twist of E if there exists an isomorphisme

$$\psi : \widetilde{E} \mapsto E$$

Exemple (E.Brier and M.Joye 2003)

Let $E : y^2 = x^3 - 3x + b$ over the field $\mathbb{F}_{p^k}$,
$\nu \in \mathbb{F}_{p^{k/2}}$ non quadratic in $\mathbb{F}_{p^{k/2}}$, such that $\sqrt{\nu} \in \mathbb{F}_{p^k}$.
Then $\widetilde{E} : \nu y^2 = x^3 - 3x + b$ over $\mathbb{F}_{p^{k/2}}$ is a twist of E,
ψ is defined by :

$$\widetilde{Q} = (x, y) \mapsto Q = (x, \sqrt{\nu} y)$$

Elimination of the denominator's evaluation

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

- $Q \in E(F_{p^k})$ is written $(x, y\sqrt{\nu})$
  where x, y, $\nu \in F_{p^{k/2}}$, $\sqrt{\nu} \in F_{p^k}$

- Consequence : $h_2 \in F_{p^{k/2}}$, so $h_2^{p^{k/2-1}} = 1$,
- For Tate : the exponent is a multiple of $p^{k/2-1}$,
- For Weil : an exponentiation to $p^{k/2-1}$ is always a pairing.

Pairing-Friendly Fields

Definition

$\mathbb{F}_{p^k}$ 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 $\mathbb{F}_{p^k}$.

Pairing-Friendly Fields

Frobenius operation

Theorem

Let ξ be a root of $X^k - \beta$,
then

$$\xi^p = \Theta.\xi \quad and \quad \xi^{p^i} = \Theta^i.\xi$$

where Θ is a constant in $\mathbb{F}_{p^k}$.

Consequence

$\omega \in \mathbb{F}^*_{p^k}$, $\omega = \sum_{i=0}^{k-1} a_i \xi^i$,

$$\omega^p = \sum_{i=0}^{k-1} a_i \Theta^i \xi^i \quad and \quad \omega^{p^j} = \sum_{i=0}^{k-1} a_i \Theta^{ij} \xi^i$$

Pairing-Friendly Fields

Tate exponentiation

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

- As n divides $\Phi_k(p)$: $\omega^{\frac{p^k-1}{n}} = \left(\omega^{\frac{p^k-1}{\Phi_k(p)}}\right)^{\frac{\Phi_k(p)}{n}}$
- The exponentiation to the power $\frac{p^k-1}{\Phi_k(p)}$ is made of Frobenius operation, so does not cost a lot.
- The more expensive operation is raising the result at the power $\frac{\Phi_k(p)}{n}$.(Lucas sequence or Sliding Signed Window)

Cyclotomic sub group

Improving the arithmetic (for Tate & Weil)

Definition

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

Lemma

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

Consequences

$\Rightarrow$ more efficient squaring.

Comparaison between Weil and Tate

Weil	Tate
Lite + Full + $Inv_{F_{p^k}}$ + $Mul_{F_{p^k}}$	Lite + expo($\frac{p^k-1}{n}$)
Lite + Full + $Mul_{F_{p^k}}$	Lite + expo($\frac{\phi_k(p)}{n}$)

Remark : $Inv_{F_{p^k}}$ uses Frobenius property, the cost can be neglected.

Characteristic p

k	coordinates	Tate exponentiation	Tate $\leq$ Weil for l.s.
2	Jacobien	Lucas sequence	≤ 128
6	Jacobien	Sliding Window Method	≤ 384
12	Jacobien	Sliding Window Method	≤ 512
24	Affine	Sliding Window Method	512...

Thank you for your attention.

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.

Remark about inversion in $\mathbb{F}_{p^k}$

Theorem

Let $\alpha \in \mathbb{F}^*_{p^k}$, the inverse of α is

$$\alpha^{-1} = \alpha^{p^{k/2}}$$

Proof

n is a prime number and n divides $p^{k/2} + 1$, so $p^{k/2} + 1 = n \times d$.

Consequence

The inversion in $\mathbb{F}_{p^k}$ is just a Frobenius operation.

Cyclotomic sub group

Improving the square

We can symboliquely compute :

$$\alpha.\alpha^{p^{k/3}} - \alpha^{p^{k/6}} = \sum_{i=0}^{k-1} v_i \xi_i$$

For $\alpha \in G_{\phi_k(p)}$, $\alpha = \sum_{i=0}^{k-1} \alpha_i \xi_i$, we have that :

$$\alpha.\alpha^{p^{k/3}} - \alpha^{p^{k/6}} = 0$$

so for all i, $v_i = 0$. Writing that :

$$\alpha^2 = \alpha^2 + \Gamma.^t \begin{bmatrix} v_0 & v_1 & v_2 & v_3 & v_4 & v_5 \end{bmatrix}$$

With a good matrix Γ the cost of the squaring is improve. For exemple, for $k = 6$, a square cost 6 multiplications.

Distorsion map.

Definition :

A not rational endomorphisme ψ from $E(\mathbb{F}_q)$ to $E(\mathbb{F}_{q^k})$.
If P is a point of order n of $E(\mathbb{F}_p)$, then $\psi(P)$ is a point of order n of $E(\mathbb{F}_{p^k})$.

Theorem :

$P \in E(\mathbb{F}_q)$ d'order r prime, $k > 1$, $E(\mathbb{F}_{q^k})$ with no points of order r^2.
Let Φ be a distorsion map, then $e(P, \Phi(P)) \neq 1$.