On compressible pairings and their computation

Michael Naehrig

Eindhoven Institute for the Protection of Systems and Information
Technische Universiteit Eindhoven
michael@cryptojedi.org

technische universiteit eindhoven

AfricaCrypt 2008, Casablanca, 13 June 2008

... joint work with
Paulo S. L. M. Barreto (University of São Paulo)
and Peter Schwabe (TU Eindhoven)

What is a pairing?

What is a pairing?

What is a pairing?

A *pairing* is a non-degenerate, bilinear map

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

where G_1, G_2 are additive groups and G_3 is written multiplicatively.

What is a pairing?

A *pairing* is a non-degenerate, bilinear map

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

where G_1, G_2 are additive groups and G_3 is written multiplicatively.

- Non-degenerate:
  for all $\mathcal{O} \neq P \in G_1$ there is a $Q \in G_2$ s.t. $e(P,Q) \neq 1$,
  for all $\mathcal{O} \neq Q \in G_2$ there is a $P \in G_1$ s.t. $e(P,Q) \neq 1$.
- Bilinear: for $P_1, P_2 \in G_1; Q_1, Q_2 \in G_2$ we have

$$\begin{aligned} e(P_1 + P_2, Q_1) &= e(P_1, Q_1)e(P_2, Q_1), \\ e(P_1, Q_1 + Q_2) &= e(P_1, Q_1)e(P_1, Q_2). \end{aligned}$$

It follows: $e(aP, bQ) = e(P,Q)^{ab} = e(bP, aQ)$.

What can be done with pairings?

Pairings on elliptic curves can be used,

- as a means to attack DL-based cryptography on groups of points on elliptic curves,
- or to construct crypto systems with certain special properties:
  - One-round tripartite key agreement,
  - Identity-based key agreement,
  - Identity-based encryption (IBE),
  - Hierarchical IBE (HIDE),
  - Short signatures (BLS).
  - much more ...

Elliptic curves

Let $p > 3$ be a prime, $\mathbb{F}_p$ the finite field with p elements and

$$E : Y^2 = X^3 + AX + B$$

an elliptic curve over $\mathbb{F}_p$.

Elliptic curves

Let $p > 3$ be a prime, $\mathbb{F}_p$ the finite field with p elements and

$$E : Y^2 = X^3 + AX + B$$

an elliptic curve over $\mathbb{F}_p$.

- $E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p^2 : y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$ is the group of $\mathbb{F}_p$-rational points on E.
  Let $n = \#E(\mathbb{F}_p)$ be its order.

Elliptic curves

Let $p > 3$ be a prime, $\mathbb{F}_p$ the finite field with p elements and

$$E : Y^2 = X^3 + AX + B$$

an elliptic curve over $\mathbb{F}_p$.

- $E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p^2 : y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$ is the group of $\mathbb{F}_p$-rational points on E.
  Let $n = \#E(\mathbb{F}_p)$ be its order.
- Let $r \neq p$ be a large prime dividing n.

Elliptic curves

Let $p > 3$ be a prime, $\mathbb{F}_p$ the finite field with p elements and

$$E : Y^2 = X^3 + AX + B$$

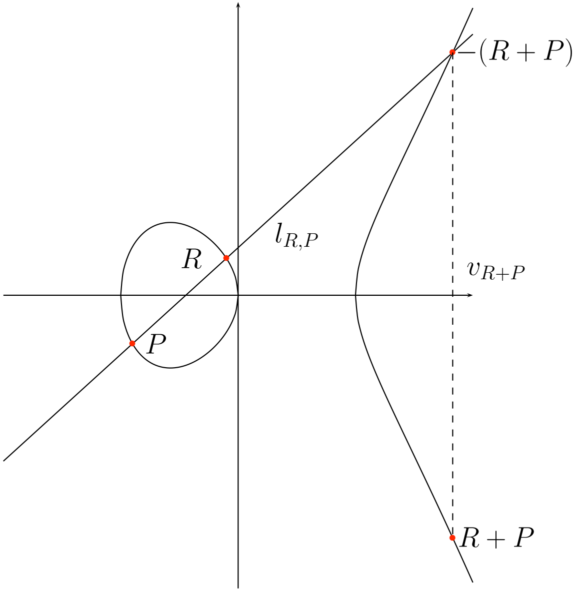
an elliptic curve over $\mathbb{F}_p$.

- $E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p^2 : y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$ is the group of $\mathbb{F}_p$-rational points on E.
  Let $n = \#E(\mathbb{F}_p)$ be its order.
- Let $r \neq p$ be a large prime dividing n.
- The *embedding degree* of E with respect to r is the smallest integer k s.t.

  $$r \mid p^k - 1 \quad \text{or equivalently} \quad r \mid \Phi_k(p),$$

  where Φ_k is the k-th cyclotomic polynomial.

Elliptic curve group law



The reduced Tate pairing

The *reduced Tate pairing* is a map

$$\begin{aligned} e : E(\mathbb{F}_p)[r] \times G_2 &\longrightarrow \mu_r \subset \mathbb{F}_{p^k}^*, \\ (P, Q) &\longmapsto f_{r,P}(Q)^{\frac{p^k-1}{r}}. \end{aligned}$$

The reduced Tate pairing

The *reduced Tate pairing* is a map

$$\begin{aligned} e : E(\mathbb{F}_p)[r] \times G_2 &\rightarrow \mu_r \subset \mathbb{F}_{p^k}^*, \\ (P, Q) &\mapsto f_{r,P}(Q)^{\frac{p^k-1}{r}}. \end{aligned}$$

- We take $G_1 = E(\mathbb{F}_p)[r]$ as the r-torsion subgroup of the group $E(\mathbb{F}_p)$, i.e. all points of order dividing r.
- $G_2 \subseteq E(\mathbb{F}_{p^k})$ is a subgroup of order r of the group of $\mathbb{F}_{p^k}$-rational points on E.
- $G_3 = \mu_r \subset \mathbb{F}_{p^k}^*$ is the group of r-th roots of unity.

The reduced Tate pairing

The *reduced Tate pairing* is a map

$$\begin{aligned} e : E(\mathbb{F}_p)[r] \times G_2 &\rightarrow \mu_r \subset \mathbb{F}_{p^k}^*, \\ (P, Q) &\mapsto f_{r,P}(Q)^{\frac{p^k-1}{r}}. \end{aligned}$$

- We take $G_1 = E(\mathbb{F}_p)[r]$ as the r-torsion subgroup of the group $E(\mathbb{F}_p)$, i.e. all points of order dividing r.
- $G_2 \subseteq E(\mathbb{F}_{p^k})$ is a subgroup of order r of the group of $\mathbb{F}_{p^k}$-rational points on E.
- $G_3 = \mu_r \subset \mathbb{F}_{p^k}^*$ is the group of r-th roots of unity.
- We obtain a unique pairing value in μ_r by raising $f_{r,P}(Q)$ to the power of $\frac{p^k-1}{r}$. This is called the *final exponentiation*.

Computing pairings (Miller's algorithm)

Input: $P \in E(\mathbb{F}_p)[r], Q \in E(\mathbb{F}_{p^k}), r = (r_m, \ldots, r_0)_2$
Output: $f_{r,P}(Q)$

$R \leftarrow P$, $f \leftarrow 1$
for $(i \leftarrow m-1;\ i \geq 0;\ i--)$ **do**
  $f \leftarrow f^2 \frac{l_{R,R}(Q)}{v_{[2]R}(Q)}$
  $R \leftarrow [2]R$
  if $(r_i = 1)$ **then**
    $f \leftarrow f \frac{l_{R,P}(Q)}{v_{R+P}(Q)}$
    $R \leftarrow R + P$
  end if
end for
return f

Compression of pairing values

Pairing values are r-th roots of unity.

- The size of r is about that of p or less.
- There are at most r different pairing values.
- Representation in $\mathbb{F}^*_{p^k}$ is redundant.
- It should be possible to have smaller representation.

Compression of pairing values

Pairing values are r-th roots of unity.

- The size of r is about that of p or less.
- There are at most r different pairing values.
- Representation in $\mathbb{F}_{p^k}^*$ is redundant.
- It should be possible to have smaller representation.

Since $r \mid \Phi_k(p)$ pairing values lie in certain subgroups of $\mathbb{F}_{p^k}^*$ (called algebraic tori).

- Granger, Page and Stam (2006) show how to use this fact to compress pairing values after the final exponentiation.
- One can do implicit multiplications in the compressed form.

Compressing certain field elements

Let k be even, $q = p^{k/2}$, $\mathbb{F}_q = \mathbb{F}_{p^{k/2}}$ and $\mathbb{F}_{q^2} = \mathbb{F}_{p^k}$ where

$$\mathbb{F}_{q^2} = \mathbb{F}_q(\sigma) = \mathbb{F}_q[X]/(X^2 - \xi).$$

- We write an element $a \in \mathbb{F}_{q^2}$ as

$$a = a_0 + a_1\sigma, \text{ where } a_0, a_1 \in \mathbb{F}_q.$$

Compressing certain field elements

Let k be even, $q = p^{k/2}$, $\mathbb{F}_q = \mathbb{F}_{p^{k/2}}$ and $\mathbb{F}_{q^2} = \mathbb{F}_{p^k}$ where

$$\mathbb{F}_{q^2} = \mathbb{F}_q(\sigma) = \mathbb{F}_q[X]/(X^2 - \xi).$$

- We write an element $a \in \mathbb{F}_{q^2}$ as

$$a = a_0 + a_1\sigma, \text{ where } a_0, a_1 \in \mathbb{F}_q.$$

- Raising such an element to the power of $q - 1$ we obtain

$$a^{q-1} = (a_0 + a_1\sigma)^{q-1} = \frac{(a_0 + a_1\sigma)^q}{a_0 + a_1\sigma} = \frac{a_0 - a_1\sigma}{a_0 + a_1\sigma}.$$

Compressing certain field elements

Let k be even, $q = p^{k/2}$, $\mathbb{F}_q = \mathbb{F}_{p^{k/2}}$ and $\mathbb{F}_{q^2} = \mathbb{F}_{p^k}$ where

$$\mathbb{F}_{q^2} = \mathbb{F}_q(\sigma) = \mathbb{F}_q[X]/(X^2 - \xi).$$

- We write an element $a \in \mathbb{F}_{q^2}$ as

$$a = a_0 + a_1\sigma, \text{ where } a_0, a_1 \in \mathbb{F}_q.$$

- Raising such an element to the power of $q - 1$ we obtain

$$a^{q-1} = (a_0 + a_1\sigma)^{q-1} = \frac{(a_0 + a_1\sigma)^q}{a_0 + a_1\sigma} = \frac{a_0 - a_1\sigma}{a_0 + a_1\sigma}.$$

- We can represent the power by just one element $\hat{a} \in \mathbb{F}_q$. For $a_1 \neq 0$ we have $\hat{a} = a_0/a_1$, i.e.

$$(a_0 + a_1\sigma)^{q-1} = \frac{a_0/a_1 - \sigma}{a_0/a_1 + \sigma} = \frac{\hat{a} - \sigma}{\hat{a} + \sigma}.$$

The final exponentiation

The exponent of the final exponentiation is

$$\frac{p^k - 1}{r} = \frac{q^2 - 1}{r} = (q-1)\frac{q+1}{r}.$$

- Thus

$$e(P,Q) = f_{r,P}(Q)^{\frac{p^k-1}{r}} = f_{r,P}(Q)^{\frac{q^2-1}{r}} = \left(f_{r,P}(Q)^{q-1}\right)^{\frac{q+1}{r}}.$$

The final exponentiation

The exponent of the final exponentiation is

$$\frac{p^k - 1}{r} = \frac{q^2 - 1}{r} = (q-1)\frac{q+1}{r}.$$

- Thus

$$e(P,Q) = f_{r,P}(Q)^{\frac{p^k-1}{r}} = f_{r,P}(Q)^{\frac{q^2-1}{r}} = \left(f_{r,P}(Q)^{q-1}\right)^{\frac{q+1}{r}}.$$

- We can do the $(q-1)$ part by just one field inversion in $\mathbb{F}_q$. Write $f_{r,P}(Q) = f = f_0 + f_1\sigma$, we can compute the compressed value of $f_{r,P}(Q)^{q-1} = f^{q-1}$ as

$$\hat{f} = f_0/f_1.$$

Multiplication of compressed elements

We would like to do implicit multiplication of compressed elements. How can we find $\widehat{ab}$ from $\hat{a}$ and $\hat{b}$? We have

$$\frac{\hat{a}-\sigma}{\hat{a}+\sigma} \cdot \frac{\hat{b}-\sigma}{\hat{b}+\sigma} = \frac{\widehat{ab}-\sigma}{\widehat{ab}+\sigma}.$$

Multiplication of compressed elements

We would like to do implicit multiplication of compressed elements. How can we find $\widehat{ab}$ from $\hat{a}$ and $\hat{b}$? We have

$$\frac{\hat{a}-\sigma}{\hat{a}+\sigma} \cdot \frac{\hat{b}-\sigma}{\hat{b}+\sigma} = \frac{\widehat{ab}-\sigma}{\widehat{ab}+\sigma}.$$

- Computing the above fraction explicitly gives

$$\widehat{ab} = (\hat{a}\hat{b}+\xi)/(\hat{a}+\hat{b}).$$

- Squaring an element is

$$\widehat{a^2} = (\hat{a}^2+\xi)/(2\hat{a}) = \hat{a}/2 + \xi/2\hat{a}.$$

- Inversion is just

$$\widehat{a^{-1}} = -\hat{a}.$$

Compressed final exponentiation

We can compress the final exponentiation by

- computing $f_{r,P}(Q)^{q-1}$ in compressed form
- and carrying out the rest of the exponentiation with implicit square-and-multiply.

Compressed final exponentiation

We can compress the final exponentiation by

- computing $f_{r,P}(Q)^{q-1}$ in compressed form
- and carrying out the rest of the exponentiation with implicit square-and-multiply.

But there is still full $\mathbb{F}_{p^k}$ arithmetic in Miller's algorithm to compute $f_{r,P}(Q)$.

Can we do the whole pairing computation in compressed form?

Miller's algorithm revisited

Input: $P \in E(\mathbb{F}_p)[r], Q \in E(\mathbb{F}_{p^k}), r = (r_m, \ldots, r_0)_2$
Output: $f_{r,P}(Q)$

$R \leftarrow P$, $f \leftarrow 1$
for $(i \leftarrow m-1;\ i \geq 0;\ i--)$ **do**
  $f \leftarrow f^2 \cdot l_{R,R}(Q)$
  $R \leftarrow [2]R$
  if $(r_i = 1)$ **then**
    $f \leftarrow f \cdot l_{R,P}(Q)$
    $R \leftarrow R + P$
  end if
end for
return f

Compressed pairing computation

To do the whole pairing computation in compressed form

- keep the variable f in compressed shape,
- do the exponentiation to $q - 1$
- and compress all values of line functions before the Miller loop.
- Multiplications of elements in $\mathbb{F}_{p^k}$ are replaced by implicit multiplications of compressed elements in $\mathbb{F}_{p^{k/2}}$.

Compressed pairings on BN curves

A BN curve is an elliptic curve with equation

$$E : Y^2 = X^3 + B$$

defined over $\mathbb{F}_p$ where $p = 36u^4 + 36u^3 + 24u^2 + 6u + 1$.

- The number n of $\mathbb{F}_p$-rational points is prime ($r = n$).
- The embedding degree of E is $k = 12$.
- BN curves have a twist of degree 6 which makes arithmetic in G_2 easier and leads to special shape of line functions.
- Pairing values lie in $\mathbb{F}^*_{p^{12}}$.

Compressed pairings on BN curves

- Split up the final exponentiation as

$$\frac{p^{12}-1}{r} = (p^6-1)(p^2+1)\frac{p^4-p^2+1}{r}.$$

- Do similar tricks as shown before to reduce an $\mathbb{F}_{p^{12}}$ element to two $\mathbb{F}_{p^2}$ elements.
- The compressed representation of the powered line functions $l_{U,V}(Q)^{(p^6-1)(p^2+1)}$ are a pair $(c_0, c_1) \in \mathbb{F}_{p^2}^2$ with

$$c_0 = \left(\frac{-\zeta_3}{1-\zeta_3^2} y_{Q'}^{-1}\right)(y_U - \lambda x_U),\ c_1 = \left(\frac{\zeta_3^2}{1-\zeta_3^2} y_{Q'}^{-1}\right)\lambda x_{Q'}.$$

Avoid finite field inversions

Finite field inversions can be completely avoided by using 'projective' representation for compressed elements.

- An inversion in $\mathbb{F}_{p^2}$ can be done by an inversion in $\mathbb{F}_p$ and some $\mathbb{F}_p$-multiplications.
- If we store one more $\mathbb{F}_p$-element we can put all inversions into that additional coordinate.
- Can compute compressed pairings using 5 instead of 12 $\mathbb{F}_p$-elements.
- No finite field inversions needed at all.

Timing results

Timing results are given for a C-implementation of pairings on the curve $E : y^2 = x^3 + 24$ over $\mathbb{F}_p$ where

$$p = 82434016654300679721217353503190038836571781 \\ 811386228921167322412819029493183 \quad (256 \text{ bits})$$

	Miller Loop	**Final Exp.**
Tate	23,350,000	9,320,000
Compressed Tate	40,650,000	11,540,000
Ate	13,520,000	9,320,000
Optimal Ate	6,750,000	9,320,000
Generalized Eta	17,370,000	9,320,000
Compressed generalized Eta	30,220,000	11,540,000

…in terms of CPU cycles on an Intel Core2 Duo T7500.

Conclusion

In this paper we have

- shown how to do pairing computation with compressed finite field elements,
- demonstrated that finite field inversions can be completely avoided during pairing computation,
- implemented compressed pairings and compared them to non-compressed pairings.

Last slide

Find a C-implementation of compressed pairings on BN curves as well as lots of other variants of pairings (based on GMP) on

`http://www.cryptojedi.org/crypto/`

Last slide

Find a C-implementation of compressed pairings on BN curves as well as lots of other variants of pairings (based on GMP) on

`http://www.cryptojedi.org/crypto/`

Find pictures of Casablanca at
`http://www.cryptojedi.org/gallery/`

Last slide

Find a C-implementation of compressed pairings on BN curves as well as lots of other variants of pairings (based on GMP) on

`http://www.cryptojedi.org/crypto/`

Find pictures of Casablanca at
`http://www.cryptojedi.org/gallery/`

Thank you for your attention!