Pairing with supersingular Trace Zero Varieties revisited

**Original**

**Availability:**
This version is available at: 11583/2373213 since:

**Publisher:**

**Published**
DOI:

**Terms of use:**
openAccess
This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

**Publisher copyright**

(Article begins on next page)
What are Trace Zero Varieties? Why Pairing on TZV?

Start with an $\eta$-hyperelectric curve $C$ over $F_q$

Trace Zero (sub)Variety of $C$ over a field ext of deg $r$:
- Subgroup of divisor class group $\text{Cl}(C/F_q)$ of $C$ over $F_q$
- Isomorphic to quotient group $(\text{Ch}(C/F_q), \text{Ch}(C/F_q))$
- Constructive application of Weil descent

Karl Rubin and Alice Silverberg in 2002, supersingularTZV:
- Allow to obtain higher MOV security per bit than EC
- Boost the security parameter by a factor of $r/\phi(r)$
- Application to pairing-based cryptography...

Transmission overhead – small :-)

\[ \text{Efficiently compute } \sigma(\alpha P) = \alpha^m(\sigma P) \text{ almost half dbls} \]

Price? Work with bigger coordinates

\[ \text{Start with genus } E \text{ with parameter greater than 6} \]

Two examples from algebraic geometry (elliptic curves)
- $E/F_q$ be an elliptic curve; $\eta$ its $\eta$-Frobenius

Embedding degree $r$ minimal such that $E[r] \subset E/F_q$

$E[r] \cong \mathbb{Z}/r \times \mathbb{Z}/r$

\[ G_1 = E[r] \cap K_1 = \mathbb{Z}/r \times \{0\} \]

\[ G_2 = E[r] \cap K_2 = \{0\} \times \mathbb{Z}/r \]

\[ P \in F_q \times E \text{, with divisor } (P) = -\mathcal{O} \]

Main result [Theorem 2]

Let $E$ be a supersingular TZV with embedding degree $r$. Suppose $r$ is even and the distortion map allows for denominator elimination. Then the Tate pairing can be computed as:

\[ e(P, Q) = \prod_{i=0}^{r-1} f_i(P)(Q^{\phi(i)})^{\alpha^{-1}} \]

where $\alpha = \frac{1}{r} \cdot M = \frac{1}{r} \cdot f_{\eta}(P)$ is the Miller function and $\phi(i)$ is a proper power of the $\eta$-Frobenius $\eta$

depends on the curve and is given in Theorem 1.

A New Algorithm for the Tate Pairing

Parallelization
- multi processors
- loop on $\sigma$

Precomputation/Storage
- $E/F_q$ points

Pairing with Supersingular TZV

$E/F_q$ be a supersingular Trace Zero Variety

A new algorithm for computing the Tate pairing $e(P, Q)$ on $E$

- Exploits the action of the $\eta$-Frobenius $\eta$
- Evaluates the Miller function $f_i(P)$ at $r$ conjugates of $Q$
- Suitable for parallel/software-friendly implementations

Survey of available algorithms in literature (extended version)
- Naturally apply to $E(F_q) \cong E$.
- Only consider the action of the $\eta$-Frobenius $\eta$

Three relevant cases (Lemmas 1, 2, 3):
- Supersingular $E_1$ over $F_{q^2}$
  - Efficient alternative (with equivalent security properties) to supersingular elliptic curves over $F_q$
- Supersingular $E_2$ over $F_{q^2}$
  - First example of supersingular abelian varieties with security parameter greater than 6
- Supersingular $E_3$ over $F_q$, $p > 3$

References

Extended version of this work: http://eprint.iacr.org/2008/404

Motivation

 WHY? To speed up the scalar multiplication
- Need to compute $[m]P$ in integer, $P$ point
- Double-and-add algorithm: $\log_m$; adds: $\frac{1}{2}\log_m$

How? Using $\eta$-Frobenius endomorphism $\eta$ (e.g. $\eta = r$)

- Efficiently compute $[m]P = \eta^m[m]P$ depends on the curve
- Scalar splitting: write $[m]P = \sum_{\delta|m} [\delta]P$, $m_0 = m_1 \ldots m_t$
- Compute concurrently $[\delta]P$ and $[\delta]P$ almost half dbls

Price? Work with bigger coordinates

- Transmission overhead – small :-)
- Point compression

\[ \text{Barreto et. al. [02–07] } \]

- Various people [06–08]: various optimisations -->
- Vercauteren [08]: optimal pairings
- Hass [08]: pairing lattices

Loop Size

| $\eta, \sigma$ | Xeon
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$E/F_q$</td>
<td>0.472</td>
</tr>
<tr>
<td>$\sigma$</td>
<td>0.983</td>
</tr>
<tr>
<td>$\eta$</td>
<td>1.506</td>
</tr>
<tr>
<td>$P$</td>
<td>1.438</td>
</tr>
<tr>
<td>$P$</td>
<td>0.775</td>
</tr>
<tr>
<td>$\eta$</td>
<td>1.375</td>
</tr>
<tr>
<td>$\sigma$</td>
<td>0.698</td>
</tr>
</tbody>
</table>