Pairing with Supersingular Trace Zero Varieties Revisited

Emanuele Cesena cesena@mat.uniroma3.it

Eurocrypt 2009

Motivation

What are Trace Zero Varieties? Why Pairing on TZV?

Proposed by Gerhard Frey in 1998. Now in *twelfth* year

Start with genus g hyperelliptic curve $\mathcal{C}$ over $\mathbb{F}_q$

Trace Zero (sub)Variety of $\mathcal{C}$ over a field ext of deg r:

- Subgroup of divisor class group $\mathrm{Cl}(\mathcal{C}/\mathbb{F}_{q^r})$ of $\mathcal{C}$ over $\mathbb{F}_{q^r}$
- Isomorphic to quotient group $\mathrm{Cl}(\mathcal{C}/\mathbb{F}_{q^r})/\mathrm{Cl}(\mathcal{C}/\mathbb{F}_q)$
- Constructive application of Weil descent

Karl Rubin and Alice Silverberg in 2002, supersingular TZV:

- 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...

Supersingular is NOT insecure!

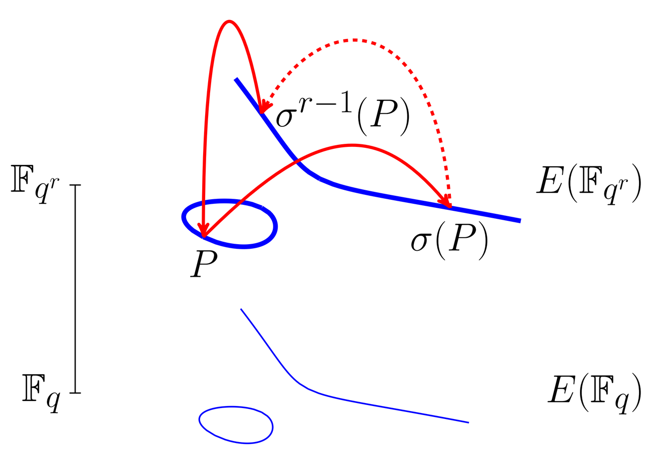
Bounded embedding degree

- Moderate security level: $<$ 1200-bit IF/DL

Symmetric pairing (distortion map)

- Much faster than asymmetric pairing

Trace Zero Varieties



$\sigma \in \mathrm{End}\,E$
$P = (x, y) \mapsto (x^q, y^q)$

Trace-zero subgroup of $E(\mathbb{F}_{q^r})$

$$E_r(\mathbb{F}_q) = \mathrm{Ker}\,\mathrm{Tr} = \{P \in E(\mathbb{F}_{q^r})\colon\ \mathrm{Tr}\,P = \mathcal{O}\}\ ,$$

where $\mathrm{Tr} = [1] + \sigma + \cdots + \sigma^{r-1} \in \mathrm{End}\,E(\mathbb{F}_{q^r})$

$E_r/\mathbb{F}_q$: subvariety of the Weil descent $\mathrm{Res}_{\mathbb{F}_{q^r}/\mathbb{F}_q} E$

Why? To speed up the scalar multiplication

- Need to compute $[m]P$ — m integer, P point
- Double-and-add algorithm — dbls: $\log m$; adds: $\frac{1}{2}\log m$

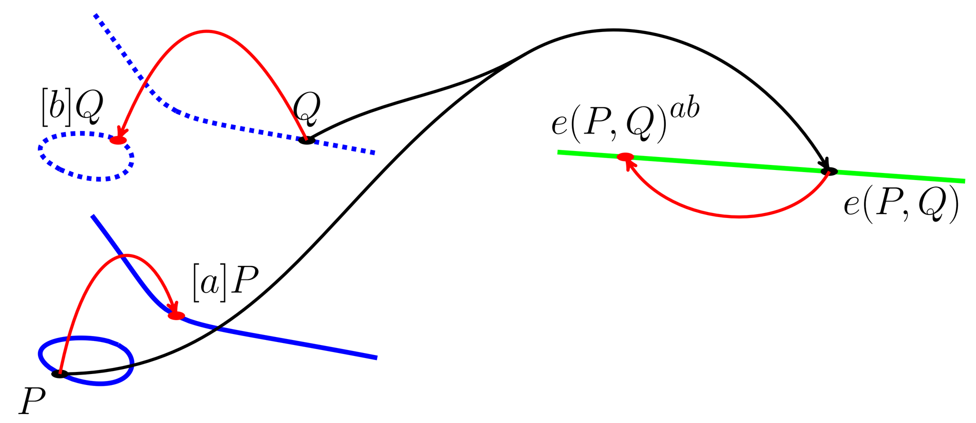
How? Using q-Frobenius endomorphism σ (e.g. $r = 3$)

- Efficiently compute $\sigma(P) = [s]P$ — s depends on the curve
- Scalar splitting: write $[m]P = [m_0 + m_1 s]P$ — $m_0, m_1 \approx \sqrt{m}$
- Compute concurrently $[m_0]P + [m_1]\sigma(P)$ — almost half dbls

Price? Work with bigger coordinates

- Transmission overhead – small :-)
- Point compression

Pairing



A new tool for cryptographers:

- $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$
- Bilinear: $e([a]P, [b]Q) = e(P,Q)^{ab}$
- Non degenerate: there exist P, Q: $e(P,Q) \neq 1$
- Efficiently computable

Two examples from algebraic geometry (elliptic curves)

- $E/\mathbb{F}_q$ be an elliptic curve; $\pi \in \mathrm{End}\,E$ be the q-Frobenius
- $l \mid \#E(\mathbb{F}_q)$ be a big prime
- Embedding degree k: minimal such that $E[l] \subset E(\mathbb{F}_{q^k})$

$$E[l] \simeq \mathbb{Z}/\mathbb{Z}_l \times \mathbb{Z}/\mathbb{Z}_l = \boxed{E[l](\mathbb{F}_q)} \times \boxed{E[l](\mathbb{F}_{q^k}) \setminus E[l](\mathbb{F}_q)}$$

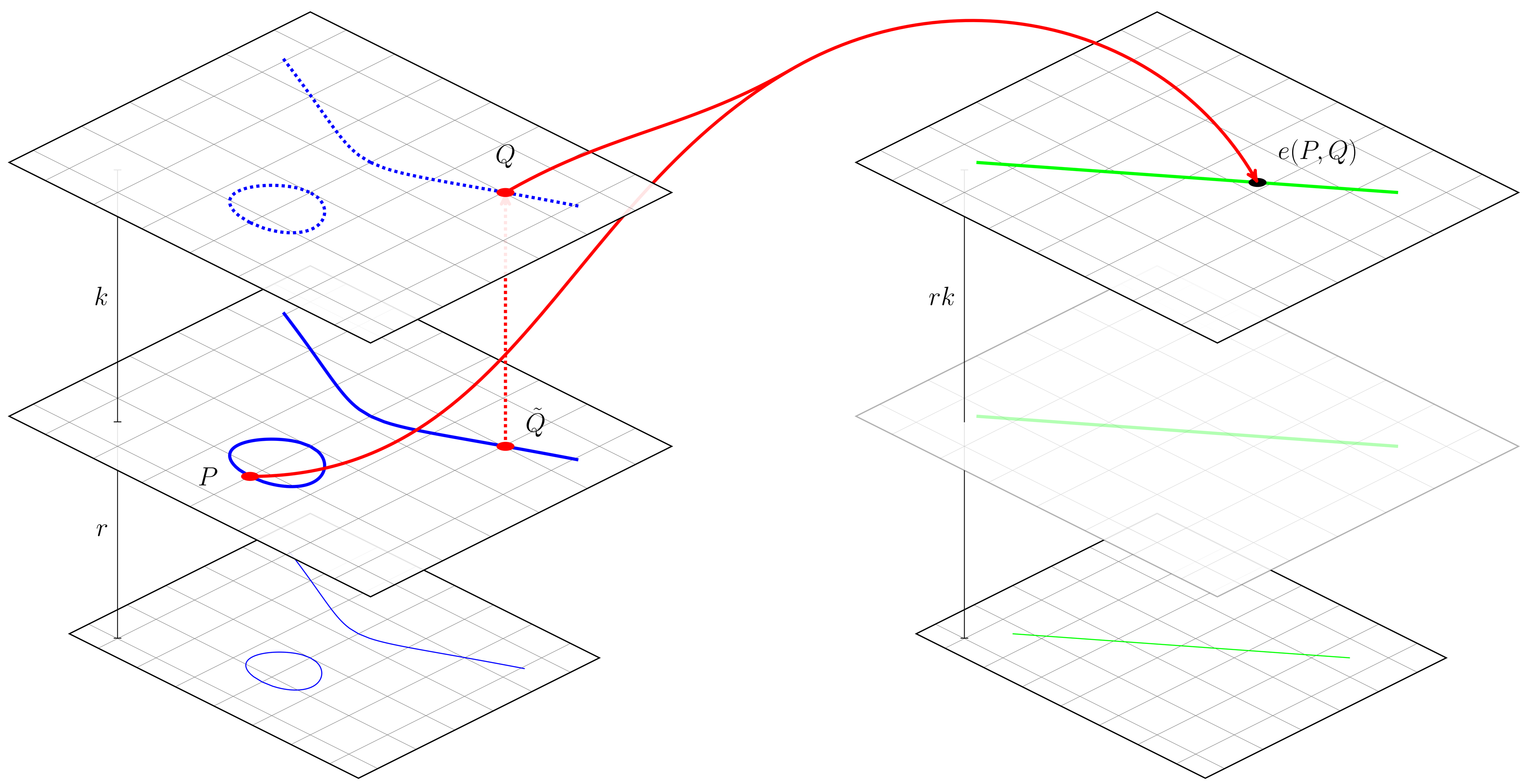
- $\boxed{\mathbb{G}_1 = E[l] \cap \mathrm{Ker}(\pi - [1])}$, $\boxed{\mathbb{G}_2 = E[l] \cap \mathrm{Ker}(\pi - [q])}$
- $\boxed{\mathbb{G}_T = \mu_l \in \mathbb{F}_{q^k}^*}$
- $f_P \in \mathbb{F}_q(E)$, with divisor $l\,(P) - l\mathcal{O}$

Weil pairing

$$w(P,Q) = \frac{f_P(Q)}{f_Q(P)}$$

Tate pairing

$$t(P,Q) = f_P(Q)^{\frac{q^k-1}{l}}$$



References

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

- Naumann [99] and Blady [02]: TZV of EC with $r = 3$, odd char
- Weimerskirch [01]: TZV of EC with $r = 5$, odd char
- Lange [03]: TZV from genus 2 HEC and $r = 3$, odd char
- Avanzi & Lange [04–07]: All three cases Implementation in odd char
- Avanzi & C. [04–07]: All three cases Implementation in even char; Next: Use of halving
- Barreto et. al. [02–07]: η and η_T with supersingular (H)EC
- Rubin & Silverberg [02–08]: supersingular AV (notably TZV)
- Scott [05]: An EC endowed with an efficient endomorphism
- Hess et. al. [06]: Ate and twisted–Ate with ordinary (H)EC
- ...various people [06-08]: various optimisations ;-)
  - Vercauteren [08]: Optimal pairings
  - Hess [08]: Pairing lattices

Abstract

Pairing with Supersingular TZV

$E_r/\mathbb{F}_q$ be a supersingular Trace Zero Variety

A new algorithm for computing the Tate pairing $t(P,Q)$ on E_r

- Exploits the action of the q-Frobenius σ
- Evaluates the Miller function $f_{q,P}$ at r conjugates of Q
- Suitable for parallel/storage-friendly implementations

Survey of available algorithms in literature (extended version)

- Naturally apply to $E(\mathbb{F}_{q^r}) \supset E_r$
- Only consider the action of the q^r-Frobenius π

Three relevant cases (Lemmas 1, 2, 3):

- Supersingular E_3 over $\mathbb{F}_{2^m}$
  Efficient alternative (with equivalent security properties) to supersingular elliptic curves over $\mathbb{F}_{3^m}$
- Supersingular E_5 over $\mathbb{F}_{3^m}$
  First example of supersingular abelian varieties with security parameter greater than 6
- Supersingular E_3 over $\mathbb{F}_p$, $p > 3$

Main result [Theorem 2]

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

$$t(P,Q) = \left(\prod_{i=0}^{r-1} f_{q,P}\left(Q^{\sigma_i}\right)^{q^{i(r+1)}}\right)^{M\frac{a}{r}q^{a-1}} \qquad ,$$

where $a = k/2$, $M = q^{k/2} - 1$, $f_{n,P}$ is the Miller function and $\sigma_i = \sigma^{ij}$ is a proper power of the q-Frobenius σ:
j depends on the curve and is given in Theorem 1.

A New Algorithm for the Tate Pairing

Parallelization

- r processors
- loop on q

Precomputation/Storage

- $\log_2 q$ points

Pairing	Loop Size	Xeon
$f_{q,P}(Q)$	$q = 2^m$	0.472
t_l	$l = O(2^{2m})$	1.983
t_N	$N = O(2^{2m})$	1.026
η	2^{3m}	1.438
η_T	$2^{(3m+1)/2} - 1$	0.775
t_{TZV}	3×2^m	1.375
t_{TZV} (par)	3×2^m	0.698

Timings (ms) on a Quad-core Xeon 3.2GHz
$E_3/\mathbb{F}_{2^{103}}\colon y^2 + y = x^3 + x + 1$

ROMA TRE UNIVERSITÀ DEGLI STUDI