PART 1
The Tate Pairing

KU LEUVEN

1

The Weil Pairing

The iconic pairing, that always helps us when we are dealing with m-torsion $E[m]$,

$$e_m : E[m] \times E[m] \to \mu_m,$$

where $\mu_m = \{ \zeta \in \overline{\mathbb{F}_q}^* \mid \zeta^m = 1 \}$. The m-Weil pairing is *bilinear, non-degenerate,* and *alternating*.

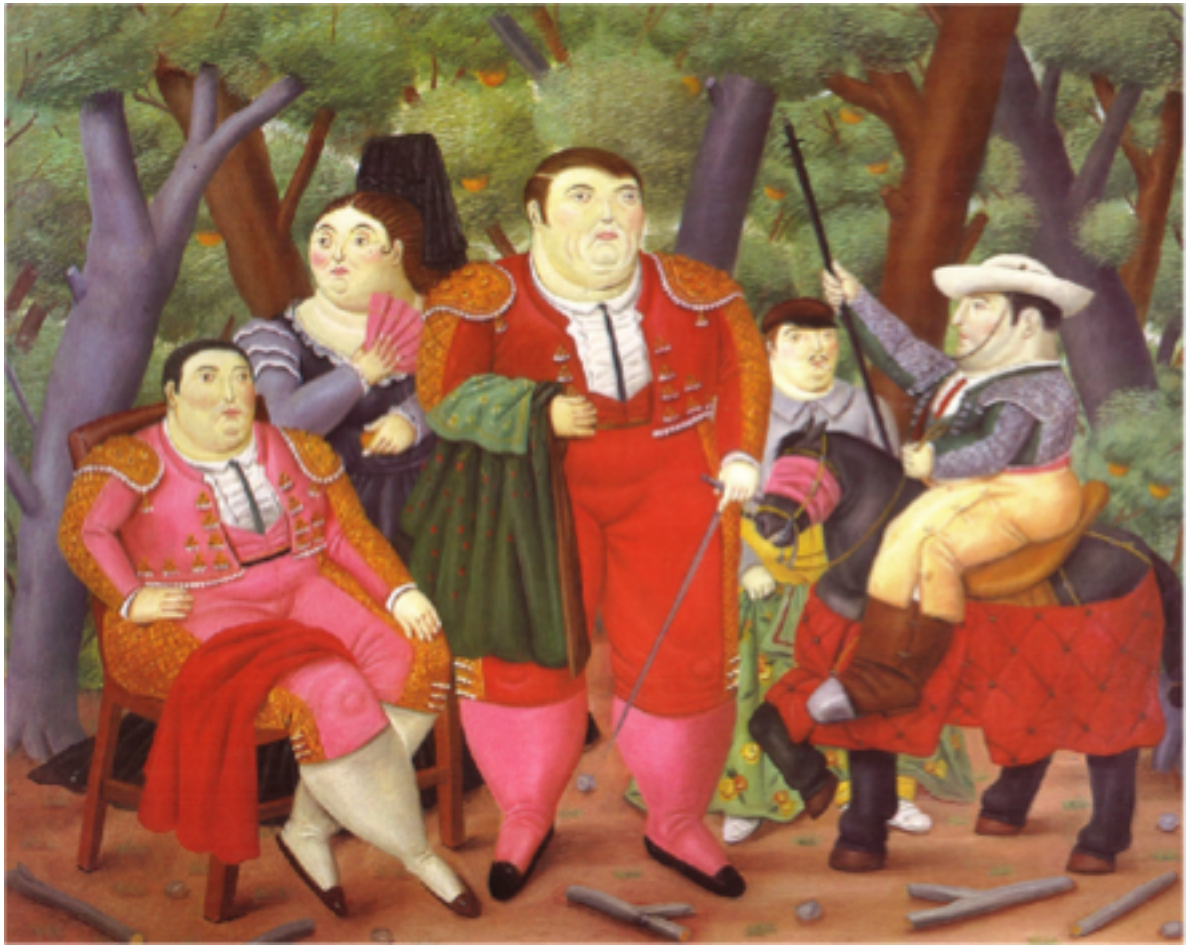
Destructive use: the MOV attack on elliptic curves, reducing elliptic-curve DLOG to $\mathbb{F}_q^*$-DLOG.

Constructive use* in isogeny-based cryptography: decomposing $K \in E[m]$ into $K = [a]P + [b]Q$ for a given basis P, Q for $E[m]$.

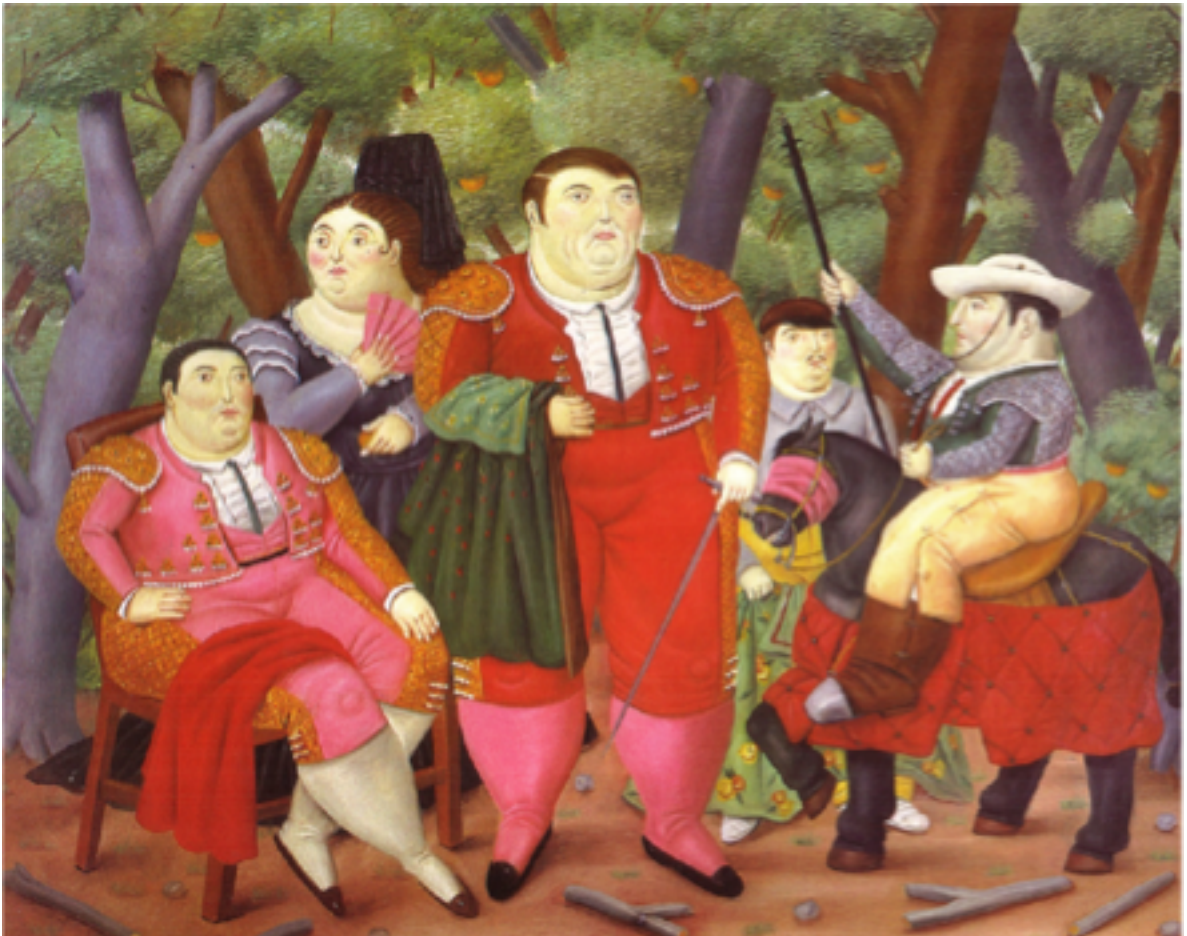
* Many other applications are out of scope for this talk, such as their uses in identity-

based cryptography and more generally the whole field of pairing-based cryptography.

Definition 3. A *pairing* on an elliptic curve E is a bilinear map $e : A \times B \to \mathbb{F}_q^*$, where A and B are subgroups of E. We say e is *non-degenerate* when for every $a \in A$, there is at least one $b \in B$ such that $e(a, b) \neq 1$, and vice versa. We say e is *alternating* when $A = B$ and for every $a \in A$ we have $e(a, a) = 1$.



Lefty and His Gang (1987)



Lefty and His Gang (1987)