The agenda for today

PART 1
The Tate Pairing

PART 2
The Tate Profile

PART 3
Generalisations

PART 1

The Tate Pairing

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)

* 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.