BLS sigs are short:

1 element of $E(\mathbb{F}_q) \approx \log_2 q$ bits

secure if $n > 2^{160}$ (DLP hard in $E(\mathbb{F}_q)$)

and $\mu_n \subset \mathbb{F}_{q^k}$, $q^k > 2^{1024}$ (DLP hard in $\mathbb{F}_{q^k}^\times$)

s/s curves over $\mathbb{F}_p$: need $p > 2^{512}$ $(k=2)$

s/s curves over $\mathbb{F}_{3^d}$: $k=6$

$q = 3^d \sim 2^{171}$, $q^6 = 2^{1024}$

Compare ECDSA or Schnorr: 2×160 bits

(1 point, 1 exponent)

What if we don't like char 3?

What if we want 128-bit security? $q \geq 2^{256}$, $q^k \geq 2^{3072}$ } want $k=12$

Ordinary pairing-friendly curves

Def: $E/\mathbb{F}_q$ is ordinary if it is not supersingular

Construction: (Cocks-Pinch): given any n & k, can find

$p \approx n^2$ & $E/\mathbb{F}_p$ s.t. $E(\mathbb{F}_p)$ has pt. of order n

& embedding degree k $(E[n] \subset E(\mathbb{F}_{p^k}))$

80-bit security: $n \approx 2^{160}$ $p \approx 2^{320}$ $k=4$ (320-bit sigs)

128-bit security: $n \approx 2^{256}$ $p \approx 2^{512}$ $k=6$ (1024-bit sigs)

We can do better in a few cases:

- Given k, want alg. to produce prime n & p & curve $\mathcal{E}/\mathbb{F}_p$ s.t. $\#\mathcal{E}(\mathbb{F}_p) = n$ and $\mathcal{E}$ has embedding degree k

Achieved for:

$k = 3, 4, 6$: Miyaji-Nakabayashi-Takano
$k = 10$: F.
$k = 12$: Barreto - Naehrig

80-bit security: $p, n \sim 2^{170}$ $k=6$ MNT curve (170-bit sigs)

128-bit security: $p, n \sim 2^{256}$ $k=12$ BN curve (256-bit sigs)

No distortion maps on ordinary curves!
$\Rightarrow$ No symmetric pairing
Use Weil pairing $e_n : G_1 \times G_2 \rightarrow \mu_n$
$G_1 = \langle P \rangle$ $P \in \mathcal{E}(\mathbb{F}_q)$ order n
$G_2 = \langle Q \rangle$ $Q \in \mathcal{E}(\mathbb{F}_{q^k}) \setminus \mathcal{E}(\mathbb{F}_q)$ order n
so $\{P, Q\}$ is basis for $\mathcal{E}[n]$

Modify BLS: $H : \{0,1\}^* \rightarrow G_1$ (small)
pk: $P, Q \in G_2$ (big)

Security "co-CDH": given $P \in G_1$; $Q, a \cdot Q \in G_2$
compute $a \cdot P$