A glimpse of hope for pairings (...in a pre-quantum world)

https://eprint.iacr.org/2018/969

Georgios Fotiadis[1] Chloe Martindale[2]

[1]University of the Aegean [2]TU Eindhoven

Early 2000s: many applications for pairings!

- Identity-based encryption
- Identity-based key exchange
- Short signatures
- ...

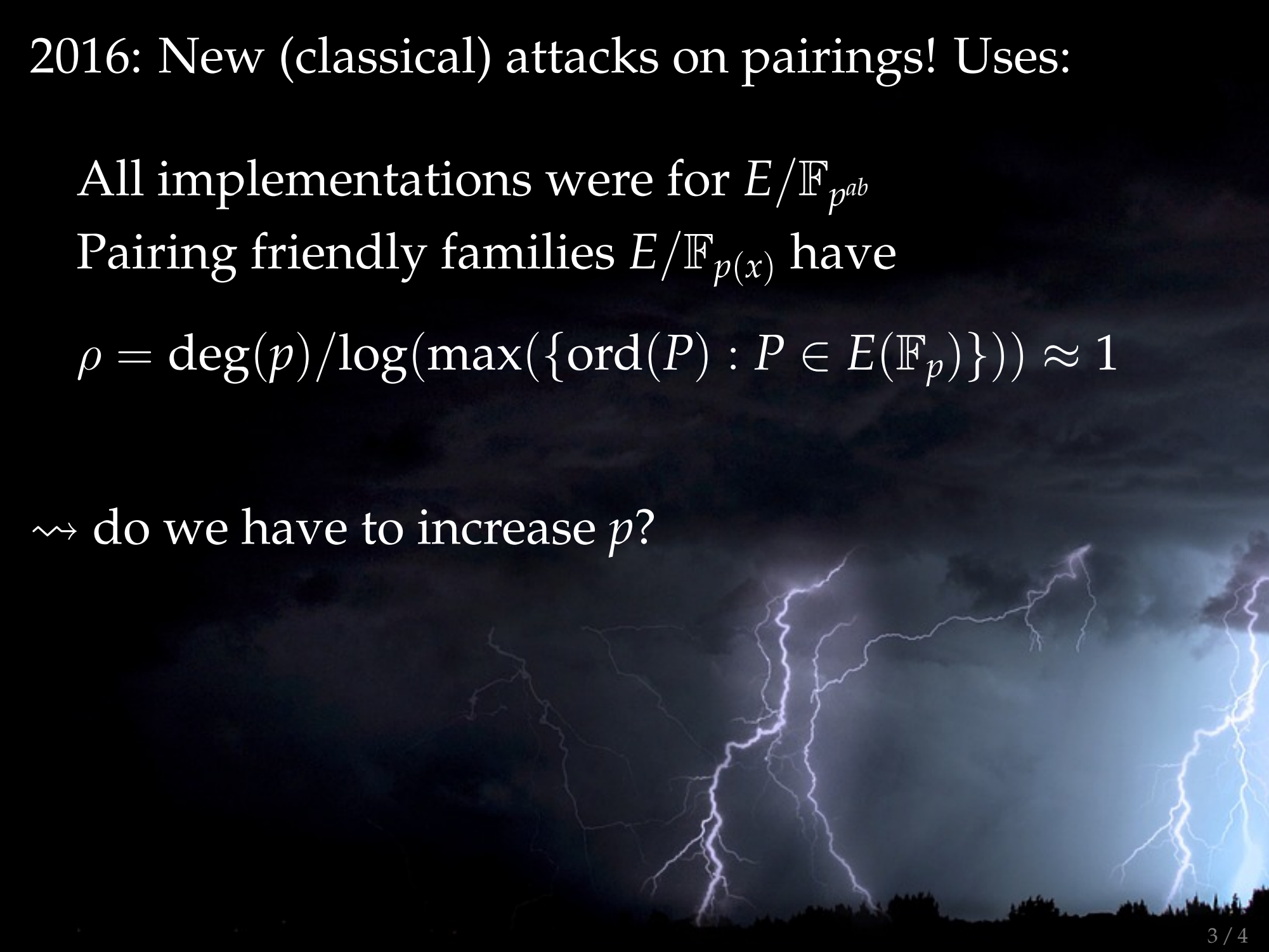
$\rightsquigarrow$ many nice constructions for families of pairing-friendly curves

2016: New (classical) attacks on pairings! Uses:

All implementations were for $E/\mathbb{F}_{p^{ab}}$
Pairing friendly families $E/\mathbb{F}_{p(x)}$ have

$$\rho = \deg(p)/\log(\max(\{\mathrm{ord}(P) : P \in E(\mathbb{F}_p)\})) \approx 1$$

$\rightsquigarrow$ do we have to increase p?



2018: Pairing constructions resistant to new attacks. Ideas:

- Increase ρ-value [1]
- Increase ab (wrt $E_{\mathbb{F}_{p^{ab}}}$)

New paper:

making an optimal secure choice of curve and pairing (uses new families)

https://eprint.iacr.org/2018/969.pdf

[1] https://eprint.iacr.org/2018/1017.pdf computes many secure families