On the performance-security relation of cryptographic pairings

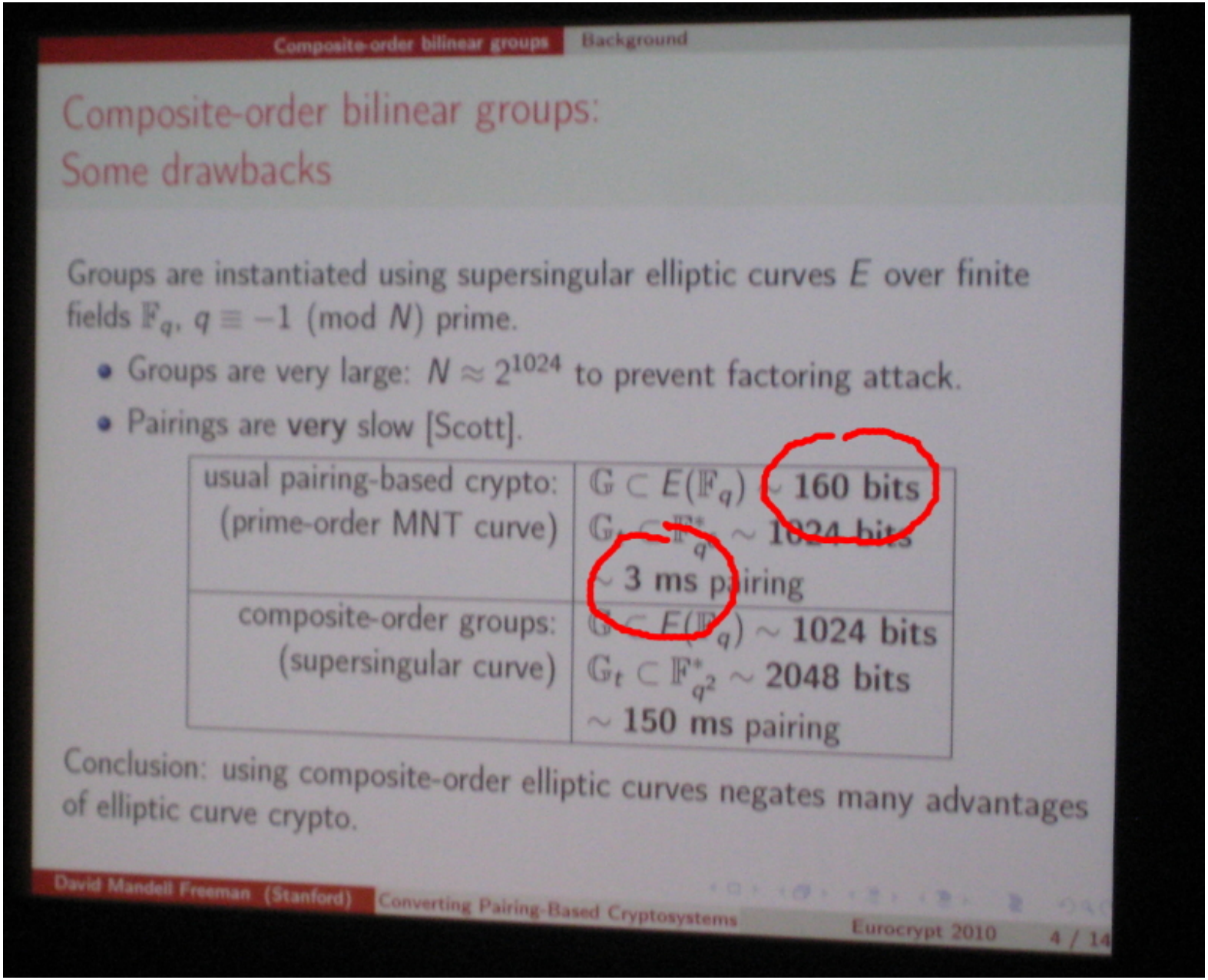
Michael Naehrig, Ruben Niederhagen, Peter Schwabe

Eindhoven University of Technology

June 1, 2010

Eurocrypt 2010 Rump Session

80-bit security pairings



128-bit security pairings

- 3 ms $\cdot \frac{128}{80} = 4.8$ ms?

128-bit security pairings

- 3 ms $\cdot \frac{128}{80} = 4.8$ ms?
- 3 ms $\cdot \left(\frac{128}{80}\right)^2 = 7.68$ ms?

128-bit security pairings

- 3 ms $\cdot \frac{128}{80} = 4.8$ ms?
- 3 ms $\cdot \left(\frac{128}{80}\right)^2 = 7.68$ ms?
- 3 ms $\cdot \left(\frac{128}{80}\right)^{1.58} = 6.31$ ms?

128-bit security pairings

- 3 ms $\cdot \frac{128}{80} = 4.8$ ms?
- 3 ms $\cdot \left(\frac{128}{80}\right)^2 = 7.68$ ms?
- 3 ms $\cdot \left(\frac{128}{80}\right)^{1.58} = 6.31$ ms?

What really happens

- Optimal ate pairing over 257-bit Barreto-Naehrig curve
- On an AMD Phenom II 955 @3210 MHz: **1.55 ms**

128-bit security pairings

- 3 ms $\cdot \frac{128}{80} = 4.8$ ms?
- 3 ms $\cdot \left(\frac{128}{80}\right)^2 = 7.68$ ms?
- 3 ms $\cdot \left(\frac{128}{80}\right)^{1.58} = 6.31$ ms?

What really happens

- Optimal ate pairing over 257-bit Barreto-Naehrig curve
- On an AMD Phenom II 955 @3210 MHz: **1.55 ms**

Questions

- How secure do we have to make pairings to get 1 ms, 0.5 ms, . . . ?

128-bit security pairings

- 3 ms $\cdot \frac{128}{80} = 4.8$ ms?
- 3 ms $\cdot \left(\frac{128}{80}\right)^2 = 7.68$ ms?
- 3 ms $\cdot \left(\frac{128}{80}\right)^{1.58} = 6.31$ ms?

What really happens

- Optimal ate pairing over 257-bit Barreto-Naehrig curve
- On an AMD Phenom II 955 @3210 MHz: **1.55 ms**

Questions

- How secure do we have to make pairings to get 1 ms, 0.5 ms, . . . ?
- Can we compute a pairing in no time with infinite security?

128-bit security pairings

- 3 ms $\cdot \frac{128}{80} = 4.8$ ms?
- 3 ms $\cdot \left(\frac{128}{80}\right)^2 = 7.68$ ms?
- 3 ms $\cdot \left(\frac{128}{80}\right)^{1.58} = 6.31$ ms?

What really happens

- Optimal ate pairing over 257-bit Barreto-Naehrig curve
- On an AMD Phenom II 955 @3210 MHz: **1.55 ms**

Questions

- How secure do we have to make pairings to get 1 ms, 0.5 ms, . . . ?
- Can we compute a pairing in no time with infinite security?
- Can we transfer this interesting relation between security and speed to other areas of cryptography?

Wanna know more?

Technische Universiteit Eindhoven University of Technology

Read our paper

New software speed records for cryptographic pairings
http://eprint.iacr.org/2010/186/

Download the code

http://cryptojedi.org/crypto/#dclxvi
(public domain)

Come to Mexico in August

Results will be presented at Latincrypt 2010.