

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

Composite-order bilinear groups Background

Composite-order bilinear groups: Some drawbacks

Groups are instantiated using supersingular elliptic curves E over finite fields \mathbb{F}_q , $q \equiv -1 \pmod{N}$ prime.

- Groups are very large: $N \approx 2^{1024}$ to prevent factoring attack.
- Pairings are very slow [Scott].

usual pairing-based crypto: (prime-order MNT curve)	$G \subset E(\mathbb{F}_q) \sim 160$ bits
	$G_t \subset \mathbb{F}_q^* \sim 1024$ bits
composite-order groups: (supersingular curve)	$G \subset E(\mathbb{F}_q) \sim 1024$ bits
	$G_t \subset \mathbb{F}_{q^2}^* \sim 2048$ bits
	~ 150 ms pairing

Conclusion: using composite-order elliptic curves negates many advantages of elliptic curve crypto.

David Mandell Freeman (Stanford) Converting Pairing-Based Cryptosystems Eurocrypt 2010 4 / 14

128-bit security pairings

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

128-bit security pairings

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

128-bit security pairings

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

128-bit security pairings

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

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

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

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

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

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

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

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?

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.