GAME OF TORSIONS

A Song of Curves and Fields

Diego F. Aranha

Department of Engineering – Aarhus University

Pairing groups

Let $\mathbb{G}_1 = \langle P \rangle$ and $\mathbb{G}_2 = \langle Q \rangle$ be r-torsion groups and $\mathbb{G}_T$ be a group of prime order r.

A general pairing

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$$

Pairings are instantiated using **families** of pairing-friendly elliptic curves, such as **BN curves** [Barreto and Naehrig, 2005].

The Realm of the Pairings [Aranha et al., 2013] established the state-of-the-art in pairing implementations for years to come.

We thought everything was fine and dandy at the realm...

Crisis in the Realm

King **Barretheo-N** is dying.

Crisis in the Realm

King **Barretheo-N** is dying. Betrayed at CRYPTO'16 by the **k-Slayer** for being too **smooth** [Kim and Barbulescu, 2016].

Crisis in the Realm

The other families in the **Realm of the Pairings** now fight for **power**.

Crisis in the Realm

The other families in the **Realm of the Pairings** now fight for **power**.

-  The **StarKSS** [Kachisa et al., 2008]

Crisis in the Realm

The other families in the **Realm of the Pairings** now fight for **power**.

-  The **StarKSS** [Kachisa et al., 2008]
-  The **BoLtonS** [Barreto et al., 2003]

Crisis in the Realm

The other families in the **Realm of the Pairings** now fight for **power**.

-  The **StarKSS** [Kachisa et al., 2008]
-  The **BoLtonS** [Barreto et al., 2003]
-  **Tullysted Hessians** [Chuengsatiansup and Martindale, 2018]

Crisis in the Realm

The other families in the **Realm of the Pairings** now fight for **power**.

-  The **StarKSS** [Kachisa et al., 2008]
-  The **BoLtonS** [Barreto et al., 2003]
-  **Tullysted Hessians** [Chuengsatiansup and Martindale, 2018]
-  The **MNTyrrels** [Miyaji et al., 2000]

Crisis in the Realm

The other families in the **Realm of the Pairings** now fight for **power**.

-  The **StarKSS** [Kachisa et al., 2008]
-  The **BoLtonS** [Barreto et al., 2003]
-  **Tullysted Hessians** [Chuengsatiansup and Martindale, 2018]
-  The **MNTyrrels** [Miyaji et al., 2000]
-  Another **Barretheo-N** over a larger field

Crisis in the Realm

The other families in the **Realm of the Pairings** now fight for **power**.

-  The **StarKSS** [Kachisa et al., 2008]
-  The **BoLtonS** [Barreto et al., 2003]
-  **Tullysted Hessians** [Chuengsatiansup and Martindale, 2018]
-  The **MNTyrrels** [Miyaji et al., 2000]
-  Another **Barretheo-N** over a larger field
-  The **Cyclotomisters** [Freeman et al., 2010]

There's more

All of this under the supernatural threat of **supersingular curves**.

There's more

All of this under the supernatural threat of **supersingular curves**.

Battle of the Brothers

Operation	BN-254	BN-382	BN-446
$e(P, Q)$ (M+F)	583+406=989	1950+1291=3241	3196+1871=5067

Table 1: Timings from RELIC in 10^3 cycles in Skylake processor measured as average of 10^4 executions (HT and TB disabled).

Battle of the Bastards

Parameters suggested by [Barbulescu and Duquesne, 2017]: curves BLS12-461 and KSS16-340.

Operation	KSS16-340	BLS12-461
$e(P, Q)$ (M+F)	1567+3856=5423	2547+2604=5151

Table 2: Timings from RELIC in 10^3 cycles in Skylake processor measured as average of 10^4 executions (HT and TB disabled).

In the Game of Torsions, either you win, or you're not cited.

dfaranha@eng.au.dk
@dfaranha
https://github.com/relic-toolkit/

References i

Aranha, D. F., Barreto, P. S. L. M., Longa, P., and Ricardini, J. E. (2013).
The realm of the pairings.
In *Selected Areas in Cryptography*, volume 8282 of *Lecture Notes in Computer Science*, pages 3–25. Springer.

Barbulescu, R. and Duquesne, S. (2017).
Updating key size estimations for pairings.
IACR Cryptology ePrint Archive, 2017:334.

Barreto, P. S. L. M., Lynn, B., and Scott, M. (2003).
On the selection of pairing-friendly groups.
In *Selected Areas in Cryptography*, volume 3006 of *Lecture Notes in Computer Science*, pages 17–25. Springer.

References ii

Barreto, P. S. L. M. and Naehrig, M. (2005).
Pairing-friendly elliptic curves of prime order.
In *Selected Areas in Cryptography*, volume 3897 of *Lecture Notes in Computer Science*, pages 319–331. Springer.

Chuengsatiansup, C. and Martindale, C. (2018).
Pairing-friendly twisted hessian curves.
IACR Cryptology ePrint Archive, 2018:1026.

Freeman, D., Scott, M., and Teske, E. (2010).
A taxonomy of pairing-friendly elliptic curves.
J. Cryptology, 23(2):224–280.

References iii

Kachisa, E. J., Schaefer, E. F., and Scott, M. (2008).
Constructing brezing-weng pairing-friendly elliptic curves using elements in the cyclotomic field.
In *Pairing*, volume 5209 of *Lecture Notes in Computer Science*, pages 126–135. Springer.

Kim, T. and Barbulescu, R. (2016).
Extended tower number field sieve: A new complexity for the medium prime case.
In *CRYPTO (1)*, volume 9814 of *Lecture Notes in Computer Science*, pages 543–571. Springer.

Miyaji, A., Nakabayashi, M., and Takano, S. (2000).
Characterization of elliptic curve traces under fr-reduction.
In *ICISC*, volume 2015 of *Lecture Notes in Computer Science*, pages 90–108. Springer.