Pairing-Friendly Twisted Hessian Curves

Chitchanok Chuengsatiansup

Inria and ENS de Lyon, France

Indocrypt, New Delhi, 11 Dec 2018

Joint work with Chloe Martindale

Pairings

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

- $\mathbb{G}_1$ and $\mathbb{G}_2$ are groups constructed from elliptic curves
- $\mathbb{G}_T$ is a multiplicative subgroup of a finite field
- all are cyclic groups of prime order r
- e is bilinear, non-degenerate, efficiently computable

Pairing groups

- $E/\mathbb{F}_q$: elliptic curve over $\mathbb{F}_q$ where q is prime
- r: largest prime factor of $n = \#E(\mathbb{F}_q) = q + 1 - t$ where t is trace of Frobenius
- k: *embedding degree* defined as smallest positive integer s.t. $r \mid (q^k - 1)$
- $\mathbb{G}_1 = E(\mathbb{F}_q)[r], \quad \mathbb{G}_2 \subseteq E(\mathbb{F}_{q^k})[r]$
- $\mathbb{G}_T = \mu_r \subseteq \mathbb{F}_{q^k}^*$ group of r-th roots of unity

Security

- attackers can attack any of $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$
- cost depends (mainly) on solving DLP
- attack algorithms: NFS and its variants, e.g., [1] [2]
- countermeasures: increase q and/or k
  - [3]: propose curve families with higher $\frac{\log q}{\log r}$
  - this paper: keep q but increase k

[1] A. Joux, C. Pierrot, *The Special Number Field Sieve in $\mathbb{F}_{p^n}$, Application to Pairing-Friendly Constructions*

[2] T. Kim and R. Barbulescu, *Extended Tower Number Field Sieve: A New Complexity for the Medium Prime Case*

[3] G. Fotiadis, E. Konstantinou, *TNFS resistant families of pairing-friendly elliptic curves*

Miller's algorithm

Algorithm 1 Miller's algorithm

Input: $m = (m_{n-1}, \ldots, m_1, m_0)_2$ and $P, Q \in E[r]$ with $P \neq Q$

Output: $e(P, Q)$

1: Initialize $R = P$ and $f = 1$
2: **for** $i := n - 2$ **down to** 0 **do**
3: $\quad f \leftarrow f^2 \cdot \ell_{2R}(Q)$ // *line function*
4: $\quad R \leftarrow 2R$ // *point doubling*
5: $\quad$ **if** $m_i = 1$ **then**
6: $\quad\quad f \leftarrow f \cdot \ell_{R,P}(Q)$ // *line function*
7: $\quad\quad R \leftarrow R + P$ // *point addition*
8: $f \leftarrow f^{(q^k-1)/r}$
9: return f

Performance of pairings

- elliptic-curve-point arithmetic:
- line function computation:
- pairing algorithm:

Performance of pairings

- elliptic-curve-point arithmetic:
  $R \leftarrow 2R, \quad R \leftarrow R + P$
- line function computation:
- pairing algorithm:

Performance of pairings

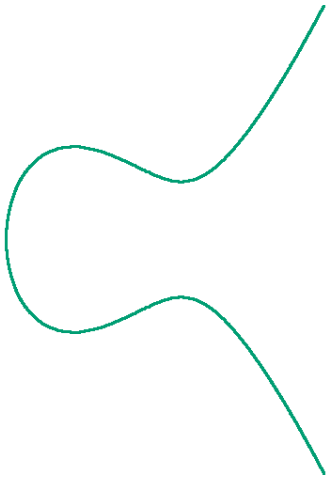
- elliptic-curve-point arithmetic:
  $R \leftarrow 2R, \quad R \leftarrow R + P$
- line function computation:
  $f \leftarrow f^2 \cdot \ell_{2R}(Q), \quad f \leftarrow f \cdot \ell_{R,P}(Q)$
- pairing algorithm:

Performance of pairings

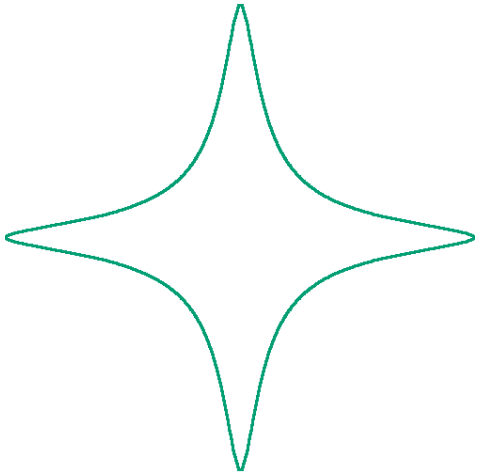
- elliptic-curve-point arithmetic:
  $R \leftarrow 2R, \quad R \leftarrow R + P$
- line function computation:
  $f \leftarrow f^2 \cdot \ell_{2R}(Q), \quad f \leftarrow f \cdot \ell_{R,P}(Q)$
- pairing algorithm: Weil, Tate, ate, ...

Curve models

Weierstrass $\mathcal{W}$

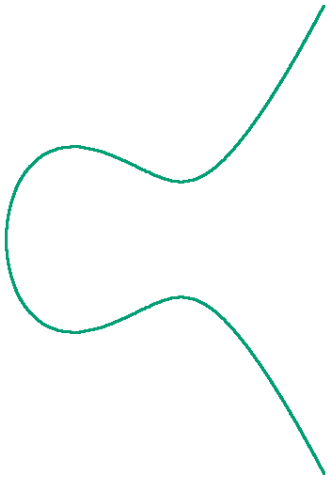


Edwards $\mathcal{E}$



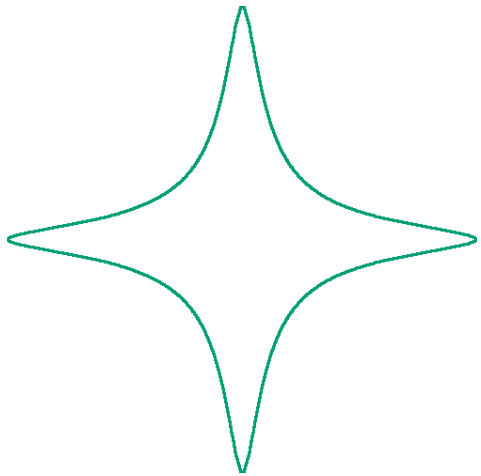
Curve models

Weierstrass $\mathcal{W}$



any elliptic curves

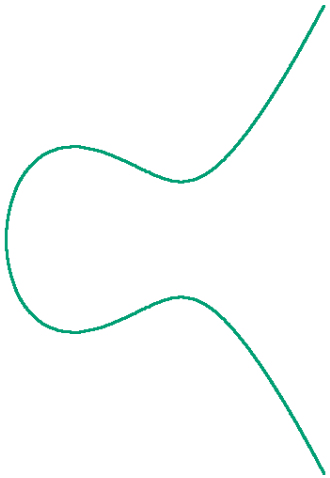
Edwards $\mathcal{E}$



need point of order 4

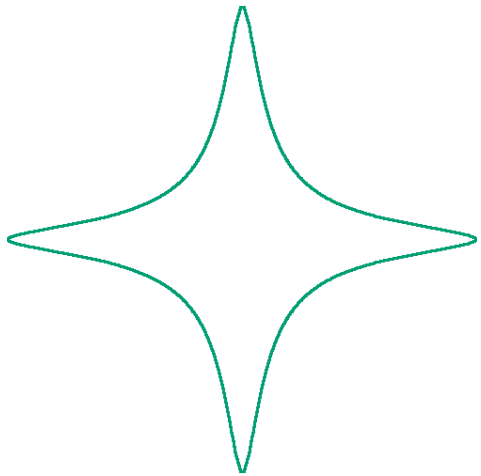
Curve models

Weierstrass $\mathcal{W}$



any elliptic curves
fast line functon

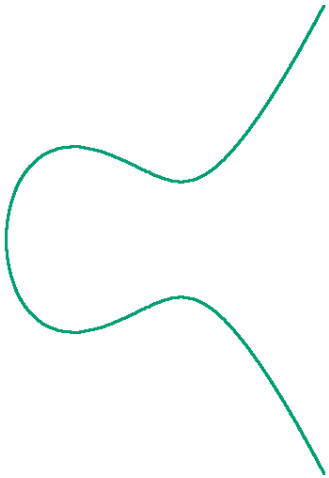
Edwards $\mathcal{E}$



need point of order 4
fast point arithmetic

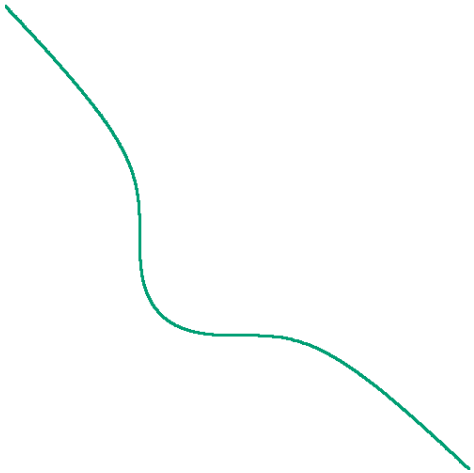
Curve models

Weierstrass $\mathcal{W}$

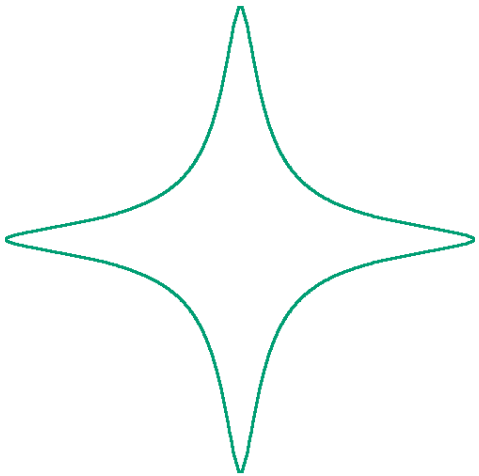


any elliptic curves
fast line functon

Hessian $\mathcal{H}$



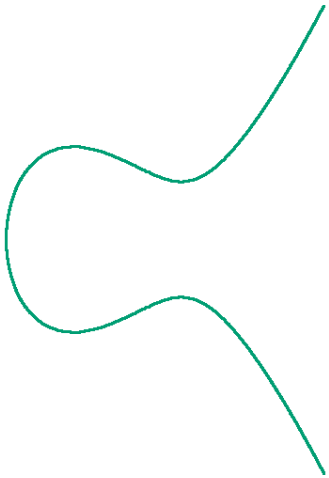
Edwards $\mathcal{E}$



need point of order 4
fast point arithmetic

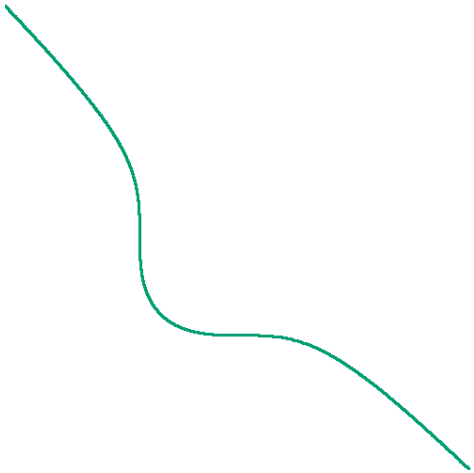
Curve models

Weierstrass $\mathcal{W}$



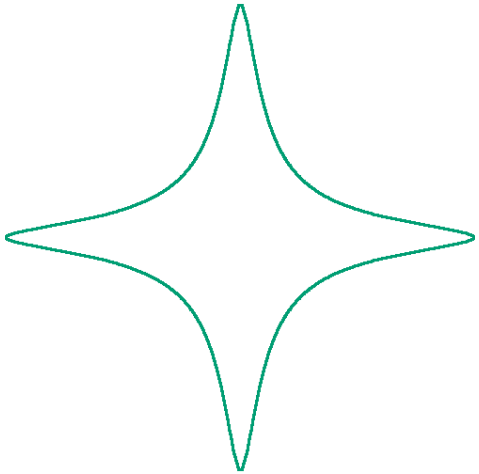
any elliptic curves
fast line functon

Hessian $\mathcal{H}$



need point of order 3

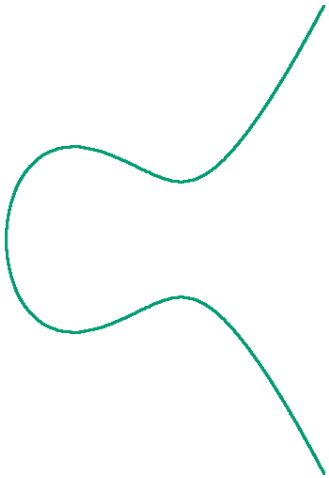
Edwards $\mathcal{E}$



need point of order 4
fast point arithmetic

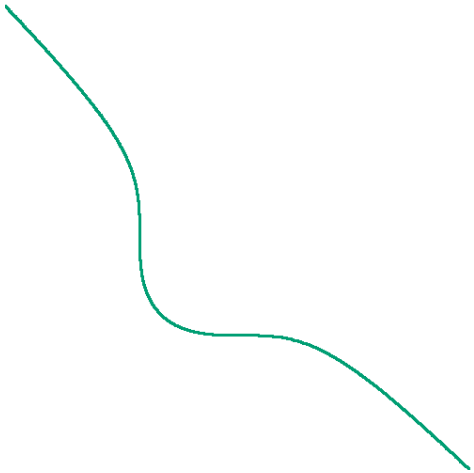
Curve models

Weierstrass $\mathcal{W}$



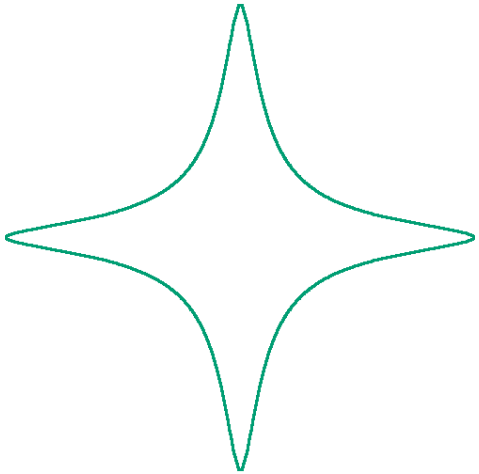
any elliptic curves
fast line functon

Hessian $\mathcal{H}$



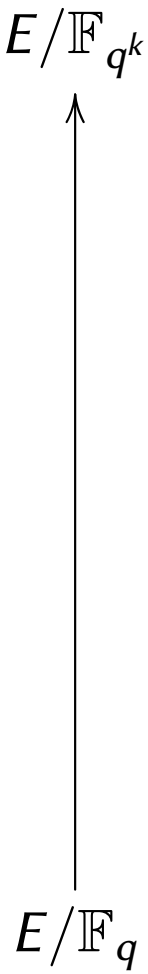
need point of order 3
???

Edwards $\mathcal{E}$

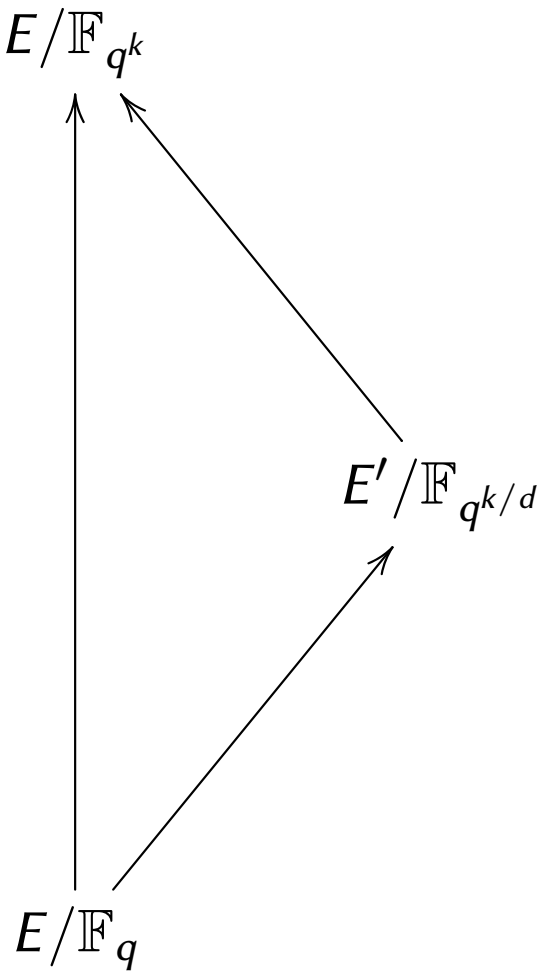


need point of order 4
fast point arithmetic

Twist of degree d



Twist of degree d



$d \in \{2, 3, 4, 6\}$

Pairings and curve models

sec level	**family-k**	$\mathbb{G}_1$	$\mathbb{G}_2$
128	BN-12	$\mathcal{W}$	$\mathcal{W}$
192	BLS-12	$\mathcal{H}$	$\mathcal{W}$
	KSS-18	$\mathcal{W}$	$\mathcal{H}$
256	BLS-24	$\mathcal{H}$	$\mathcal{E}$

Pairings and curve models

sec level	**family-k**	$\mathbb{G}_1$	$\mathbb{G}_2$
128	BN-12	$\mathcal{W}$	$\mathcal{W}$
	???	$\mathcal{H}$	$\mathcal{H}$
192	BLS-12	$\mathcal{H}$	$\mathcal{W}$
	KSS-18	$\mathcal{W}$	$\mathcal{H}$
	???	$\mathcal{H}$	$\mathcal{H}$
256	BLS-24	$\mathcal{H}$	$\mathcal{E}$

Curve constructions

- $k \equiv 3 \pmod{18}$ (see [1], Construction 6.6)
- $k \equiv 9, 15 \pmod{18}$ (see [1], Construction 6.6)
- $k \equiv 0 \pmod{6}$ and $18 \nmid k$ (see [1], Construction 6.6)

[1] D. Freeman, M. Scott and E. Teske, *A Taxonomy of Pairing-Friendly Elliptic Curves*

Curve constructions

- $k \equiv 3 \pmod{18}$ (see [1], Construction 6.6)
  e.g., $k = 21$
- $k \equiv 9, 15 \pmod{18}$ (see [1], Construction 6.6)
  e.g., $k = 15$
- $k \equiv 0 \pmod{6}$ and $18 \nmid k$ (see [1], Construction 6.6)
  e.g., $k = 12, 24$

[1] D. Freeman, M. Scott and E. Teske, *A Taxonomy of Pairing-Friendly Elliptic Curves*

Curve constructions

- $k \equiv 3 \pmod{18}$ (see [1], Construction 6.6)
  e.g., $k = 21$
  192-bit: $\log r \approx 420$, $\log q \approx 560$, $k \log q \approx 11760$

- $k \equiv 9, 15 \pmod{18}$ (see [1], Construction 6.6)
  e.g., $k = 15$

- $k \equiv 0 \pmod{6}$ and $18 \nmid k$ (see [1], Construction 6.6)
  e.g., $k = 12, 24$

[1] D. Freeman, M. Scott and E. Teske, *A Taxonomy of Pairing-Friendly Elliptic Curves*

Curve constructions

- $k \equiv 3 \pmod{18}$ (see [1], Construction 6.6)
  e.g., $k = 21$
  192-bit: $\log r \approx 420$, $\log q \approx 560$, $k \log q \approx 11760$

- $k \equiv 9, 15 \pmod{18}$ (see [1], Construction 6.6)
  e.g., $k = 15$
  143-bit: $\log r \approx 256$, $\log q \approx 384$, $k \log q \approx 5760$

- $k \equiv 0 \pmod{6}$ and $18 \nmid k$ (see [1], Construction 6.6)
  e.g., $k = 12, 24$

[1] D. Freeman, M. Scott and E. Teske, *A Taxonomy of Pairing-Friendly Elliptic Curves*

Curve constructions

- $k \equiv 3 \pmod{18}$ (see [1], Construction 6.6)
  e.g., $k = 21$
  192-bit: $\log r \approx 420$, $\log q \approx 560$, $k \log q \approx 11760$

- $k \equiv 9, 15 \pmod{18}$ (see [1], Construction 6.6)
  e.g., $k = 15$
  143-bit: $\log r \approx 256$, $\log q \approx 384$, $k \log q \approx 5760$

- $k \equiv 0 \pmod{6}$ and $18 \nmid k$ (see [1], Construction 6.6)
  e.g., $k = 12, 24$
  192-bit (with $k = 24$): $\log r \approx 392$, $\log q \approx 490$, $k \log q \approx 11760$

[1] D. Freeman, M. Scott and E. Teske, *A Taxonomy of Pairing-Friendly Elliptic Curves*

Comparison

Best known timings for $k = 12, 15, 21, 24$

k	**pairing**	**model**	**# iterations**	**DBLc**	**ADDc**
12	twisted ate	Edwards [1]	$\log(r)/3$	62.9	25.3
	optimal ate	Projective [2]	$\log(r)/4$	73.8	49.6
	optimal ate	Hessian (this paper)	$\log(r)/4$	73.5	66.0
15	twisted ate	Projective [2]	$\log(r)$	431.6	255.4
	optimal ate	Hessian (this paper)	$\log(r)/8$	103.1	120.0
21	twisted ate	Projective [2]	$\log(r)$	826.4	477.4
	optimal ate	Hessian (this paper)	$\log(r)/12$	133.8	155.9
24	twisted ate	Edwards [1]	$\log(r)/3$	231.5	78.7
	optimal ate	Projective [2]	$\log(r)/8$	147.5	99.2
	optimal ate	Hessian (this paper)	$\log(r)/8$	140.7	134.0

[1] L. Li, H. Wu, F. Zhang, *"Pairing Computation on Edwards Curves with High-Degree Twists"*.
[2] C. Costello, H. Hisil, C. Boyd, J. M. González Nieto, K. K-H. Wong, *"Faster Pairings on Special Weierstrass Curves"*.

Summary

- constructions of pairing-friendly (twisted) Hessian curves
- exploitation of degree-3 twist on $\mathcal{H}$
- efficient formulas for $\mathbb{G}_1 \times \mathbb{G}_2$ and $\mathbb{G}_2 \times \mathbb{G}_1$ pairings on $\mathcal{H}$
- security analysis for 128- and 192-bit security
- fastest known pairing for $k = 15$ and $k = 21$