Cocks–Pinch curves with efficient ate pairing

Simon Masson
Joint work with A. Guillevic, E. Thomé

Journées C2

October 9, 2018

Pairings on elliptic curves

Definition

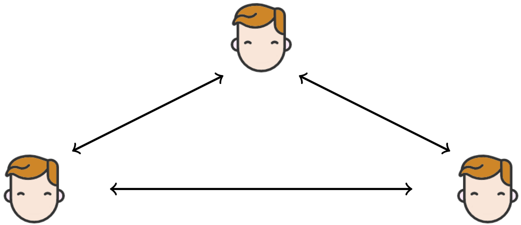
A pairing on an elliptic curve E is a bilinear non-degenerate application $e : E \times E \longrightarrow \mathbb{F}_{p^k}^{\times}$

Pairings on elliptic curves

Definition

A pairing on an elliptic curve E is a bilinear non-degenerate application $e : E \times E \longrightarrow \mathbb{F}_{p^k}^{\times}$

Tripartite one round key exchange. (Joux 2000)

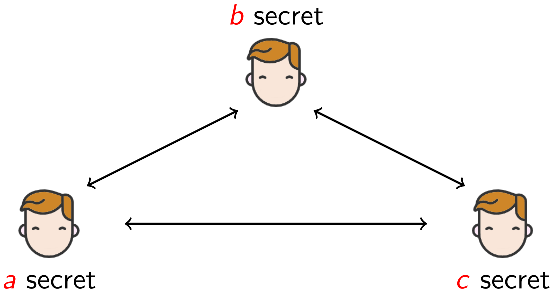


Pairings on elliptic curves

Definition

A pairing on an elliptic curve E is a bilinear non-degenerate application $e : E \times E \longrightarrow \mathbb{F}_{p^k}^{\times}$

Tripartite one round key exchange. (Joux 2000)

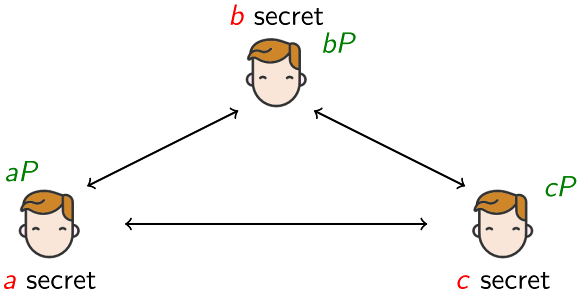


Pairings on elliptic curves

Definition

A pairing on an elliptic curve E is a bilinear non-degenerate application $e : E \times E \longrightarrow \mathbb{F}_{p^k}^{\times}$

Tripartite one round key exchange. (Joux 2000)

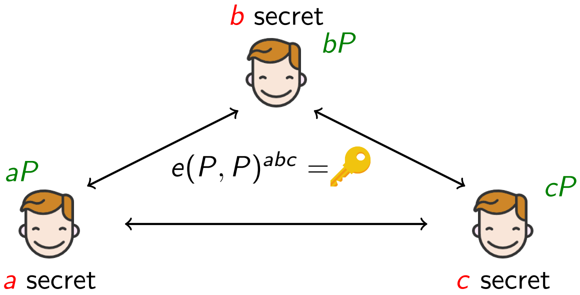


Pairings on elliptic curves

Definition

A pairing on an elliptic curve E is a bilinear non-degenerate application
$e : E \times E \longrightarrow \mathbb{F}_{p^k}^{\times}$

Tripartite one round key exchange. (Joux 2000)



Tate and ate pairing

Definition

The Miller loop computes the function $f_{s,Q}$ such that Q is a zero of order s, and $[s]Q$ is a pole of order 1, i.e

$$\mathrm{div}(f_{s,Q}) = s(Q) - ([s]Q) - (s-1)\mathcal{O}$$

Definition

For $P, Q \in E[r]$ such that $\pi_p(P) = P$, $\pi_p(Q) = [p]Q$,

$$\mathrm{Tate}(P,Q) := f_{r,P}(Q)^{(p^k-1)/r} \qquad \mathrm{ate}(P,Q) := f_{t-1,Q}(P)^{(p^k-1)/r}$$

Definition

The Miller loop computes the function $f_{s,Q}$ such that Q is a zero of order s, and $[s]Q$ is a pole of order 1, i.e

$$\mathrm{div}(f_{s,Q}) = s(Q) - ([s]Q) - (s-1)\mathcal{O}$$

Definition

For $P, Q \in E[r]$ such that $\pi_p(P) = P$, $\pi_p(Q) = [p]Q$,

$$\mathrm{Tate}(P,Q) := f_{r,P}(Q)^{(p^k-1)/r} \qquad \mathrm{ate}(P,Q) := f_{t-1,Q}(P)^{(p^k-1)/r}$$

For ate:

1. Compute $x = f_{t-1,Q}(P)$ (Miller loop) with $P \in E(\mathbb{F}_p)[r]$ and $Q \in E(\mathbb{F}_{p^k})[r]$

Definition

The Miller loop computes the function $f_{s,Q}$ such that Q is a zero of order s, and $[s]Q$ is a pole of order 1, i.e

$$\mathrm{div}(f_{s,Q}) = s(Q) - ([s]Q) - (s-1)\mathcal{O}$$

Definition

For $P, Q \in E[r]$ such that $\pi_p(P) = P$, $\pi_p(Q) = [p]Q$,

$$\mathrm{Tate}(P,Q) := f_{r,P}(Q)^{(p^k-1)/r} \qquad \mathrm{ate}(P,Q) := f_{t-1,Q}(P)^{(p^k-1)/r}$$

For ate:

1. Compute $x = f_{t-1,Q}(P)$ (Miller loop) with $P \in E(\mathbb{F}_p)[r]$ and $Q \in E(\mathbb{F}_{p^k})[r]$
2. Compute $x^{(p^k-1)/r}$ (final exponentiation)

Algorithm: $\textsc{MillerLoop}(s, P, Q)$ – Compute $f_{s,Q}(P)$.

$f \leftarrow 1$
$S \leftarrow Q$
for b bit of s from second MSB to LSB **do**
  $f \leftarrow f^2 \cdot \ell_{S,S}(P)/v_{2S}(P)$
  $S \leftarrow [2]S$
  if $b = 1$ **then**
    $f \leftarrow f \cdot \ell_{S,Q}(P)/v_{S+Q}(P)$
    $S \leftarrow S + Q$
  end if
end for
return f such that $\mathrm{div}(f_{s,Q}) = s(Q) - ([s]Q) - (s-1)\mathcal{O}$

Example: $f_{5,Q}(P)$.

$$s = 5 = \overline{101}^{2}$$

Example: $f_{5,Q}(P)$.

$$s = 5 = \overline{\boxed{1}01}^{2}$$

$$f = 1$$

Example: $f_{5,Q}(P)$.

$$s = 5 = \overline{1\boxed{0}1}^{2}$$

$$f = 1$$

Example: $f_{5,Q}(P)$.

$$s = 5 = \overline{1\boxed{0}1}^{2}$$

$$f = 1^2$$

Example: $f_{5,Q}(P)$.

$$s = 5 = \overline{1\boxed{0}1}^{2}$$

$$f = 1^2 \cdot \ell_{Q,Q}(P)/v_{2Q}(P)$$

Example: $f_{5,Q}(P)$.

$$s = 5 = \overline{10\boxed{1}}^{2}$$

$$f = \left(1^2 \cdot \ell_{Q,Q}(P)/v_{2Q}(P)\right)^2$$

Example: $f_{5,Q}(P)$.

$$s = 5 = \overline{10\boxed{1}}^{2}$$

$$f = \left(1^2 \cdot \ell_{Q,Q}(P)/v_{2Q}(P)\right)^2 \cdot \ell_{2Q,2Q}(P)/v_{4Q}(P)$$

Example: $f_{5,Q}(P)$.

$$s = 5 = \overline{10\boxed{1}}^{2}$$

$$f = \left(1^2 \cdot \ell_{Q,Q}(P)/v_{2Q}(P)\right)^2 \cdot \ell_{2Q,2Q}(P)/v_{4Q}(P) \cdot \ell_{4Q,Q}(P)/v_{5Q}(P)$$

Example: $f_{5,Q}(P)$.

$$s = 5 = \overline{101}^2$$

$$f = \left(1^2 \cdot \ell_{Q,Q}(P)/v_{2Q}(P)\right)^2 \cdot \ell_{2Q,2Q}(P)/v_{4Q}(P) \cdot \ell_{4Q,Q}(P)/v_{5Q}(P)$$

Divisor:

$$4(Q) + 2(-2Q)$$

Example: $f_{5,Q}(P)$.

$$s = 5 = \overline{101}^2$$

$$f = \left(1^2 \cdot \ell_{Q,Q}(P)/v_{2Q}(P)\right)^2 \cdot \ell_{2Q,2Q}(P)/v_{4Q}(P) \cdot \ell_{4Q,Q}(P)/v_{5Q}(P)$$

Divisor:

$$4(Q) + 2(-2Q) + 2(2Q) + (-4Q)$$

Example: $f_{5,Q}(P)$.

$$s = 5 = \overline{101}^2$$

$$f = \left(1^2 \cdot \ell_{Q,Q}(P)/v_{2Q}(P)\right)^2 \cdot \ell_{2Q,2Q}(P)/v_{4Q}(P) \cdot \ell_{4Q,Q}(P)/v_{5Q}(P)$$

Divisor:

$$4(Q) + 2(-2Q) + 2(2Q) + (-4Q) + (Q) + (4Q) + (-5Q)$$

Example: $f_{5,Q}(P)$.

$$s = 5 = \overline{101}^2$$

$$f = \left(1^2 \cdot \ell_{Q,Q}(P)/v_{2Q}(P)\right)^2 \cdot \ell_{2Q,2Q}(P)/v_{4Q}(P) \cdot \ell_{4Q,Q}(P)/v_{5Q}(P)$$

Divisor:

$$4(Q) + 2(-2Q) + 2(2Q) + (-4Q) + (Q) + (4Q) + (-5Q)$$

$$-2(2Q) - 2(-2Q) - 2(\mathcal{O})$$

Example: $f_{5,Q}(P)$.

$$s = 5 = \overline{101}^2$$

$$f = \left(1^2 \cdot \ell_{Q,Q}(P)/v_{2Q}(P)\right)^2 \cdot \ell_{2Q,2Q}(P)/v_{4Q}(P) \cdot \ell_{4Q,Q}(P)/v_{5Q}(P)$$

Divisor:

$$4(Q) + 2(-2Q) + 2(2Q) + (-4Q) + (Q) + (4Q) + (-5Q)$$

$$-2(2Q) - 2(-2Q) - 2(\mathcal{O}) - (4Q) - (-4Q) - (\mathcal{O})$$

Example: $f_{5,Q}(P)$.

$$s = 5 = \overline{101}^2$$

$$f = \left(1^2 \cdot \ell_{Q,Q}(P)/v_{2Q}(P)\right)^2 \cdot \ell_{2Q,2Q}(P)/v_{4Q}(P) \cdot \ell_{4Q,Q}(P)/v_{5Q}(P)$$

Divisor:

$$4(Q) + 2(-2Q) + 2(2Q) + (-4Q) + (Q) + (4Q) + (-5Q)$$

$$-2(2Q) - 2(-2Q) - 2(\mathcal{O}) - (4Q) - (-4Q) - (\mathcal{O}) - (5Q) - (-5Q) - (\mathcal{O})$$

Example: $f_{5,Q}(P)$.

$$s = 5 = \overline{101}^2$$

$$f = \left(1^2 \cdot \ell_{Q,Q}(P)/v_{2Q}(P)\right)^2 \cdot \ell_{2Q,2Q}(P)/v_{4Q}(P) \cdot \ell_{4Q,Q}(P)/v_{5Q}(P)$$

Divisor:

$$4(Q) + 2(-2Q) + 2(2Q) + (-4Q) + (Q) + (4Q) + (-5Q)$$

$$-2(2Q) - 2(-2Q) - 2(\mathcal{O}) - (4Q) - (-4Q) - (\mathcal{O}) - (5Q) - (-5Q) - (\mathcal{O})$$

$$\mathrm{div}(f) = 5(Q) - (5Q) - 4(\mathcal{O})$$

The final exponentiation is $(f_{t-1,Q}(P))^{\frac{p^k-1}{r}}$

The final exponentiation is $(f_{t-1,Q}(P))^{\frac{p^k-1}{r}}$

Proposition

For x in a subfield of $\mathbb{F}_{p^k}^\times$, $x^{\frac{p^k-1}{r}} = 1$.

The final exponentiation is $(f_{t-1,Q}(P))^{\frac{p^k-1}{r}}$

Proposition

For x in a subfield of $\mathbb{F}_{p^k}^\times$, $x^{\frac{p^k-1}{r}} = 1$.

- When k is even, say $\mathbb{F}_{p^k} = \mathbb{F}_{p^{k/2}}(u)$.
  $E(\mathbb{F}_{p^k})[r] \simeq E'(\mathbb{F}_{p^{k/2}})[r] \Longrightarrow P = (x, yu)$ with $x, y \in \mathbb{F}_{p^{k/2}}$.

The final exponentiation is $(f_{t-1,Q}(P))^{\frac{p^k-1}{r}}$

Proposition

For x in a subfield of $\mathbb{F}_{p^k}^{\times}$, $x^{\frac{p^k-1}{r}} = 1$.

- When k is even, say $\mathbb{F}_{p^k} = \mathbb{F}_{p^{k/2}}(u)$.
  $E(\mathbb{F}_{p^k})[r] \simeq E'(\mathbb{F}_{p^{k/2}})[r] \implies P = (x, yu)$ with $x, y \in \mathbb{F}_{p^{k/2}}$.
  Vertical lines $v_S(P) \in \mathbb{F}_{p^{k/2}}$ 

The final exponentiation is $(f_{t-1,Q}(P))^{\frac{p^k-1}{r}}$

Proposition

For x in a subfield of $\mathbb{F}_{p^k}^{\times}$, $x^{\frac{p^k-1}{r}} = 1$.

- When k is even, say $\mathbb{F}_{p^k} = \mathbb{F}_{p^{k/2}}(u)$.
  $E(\mathbb{F}_{p^k})[r] \simeq E'(\mathbb{F}_{p^{k/2}})[r] \Longrightarrow P = (x, yu)$ with $x, y \in \mathbb{F}_{p^{k/2}}$.
  Vertical lines $v_S(P) \in \mathbb{F}_{p^{k/2}}$ 
- When $4 \mid k$ and $b = 0$ or $6 \mid k$ and $a = 0$, line computations are more efficient 

The final exponentiation is $(f_{t-1,Q}(P))^{\frac{p^k-1}{r}}$

Proposition

For x in a subfield of $\mathbb{F}_{p^k}^\times$, $x^{\frac{p^k-1}{r}} = 1$.

- When k is even, say $\mathbb{F}_{p^k} = \mathbb{F}_{p^{k/2}}(u)$.
  $E(\mathbb{F}_{p^k})[r] \simeq E'(\mathbb{F}_{p^{k/2}})[r] \Longrightarrow P = (x, yu)$ with $x, y \in \mathbb{F}_{p^{k/2}}$.
  Vertical lines $v_S(P) \in \mathbb{F}_{p^{k/2}}$
- When $4 \mid k$ and $b = 0$ or $6 \mid k$ and $a = 0$, line computations are more efficient

$$f = \left(1^2 \cdot \ell_{Q,Q}(P)/v_{2Q}(P)\right)^2 \cdot \ell_{2Q,2Q}(P)/v_{4Q}(P) \cdot \ell_{4Q,Q}(P)/v_{5Q}(P)$$

The final exponentiation is $(f_{t-1,Q}(P))^{\frac{p^k-1}{r}}$

Proposition

For x in a subfield of $\mathbb{F}_{p^k}^\times$, $x^{\frac{p^k-1}{r}} = 1$.

- When k is even, say $\mathbb{F}_{p^k} = \mathbb{F}_{p^{k/2}}(u)$.
  $E(\mathbb{F}_{p^k})[r] \simeq E'(\mathbb{F}_{p^{k/2}})[r] \Longrightarrow P = (x, yu)$ with $x, y \in \mathbb{F}_{p^{k/2}}$.
  Vertical lines $v_S(P) \in \mathbb{F}_{p^{k/2}}$
- When $4 \mid k$ and $b = 0$ or $6 \mid k$ and $a = 0$, line computations are more efficient

$$f = \left(1^2 \cdot \ell_{Q,Q}(P)/v_{2Q}(P)\right)^2 \cdot \ell_{2Q,2Q}(P)/v_{4Q}(P) \cdot \ell_{4Q,Q}(P)/v_{5Q}(P)$$

The final exponentiation is $(f_{t-1,Q}(P))^{\frac{p^k-1}{r}}$

Proposition

For x in a subfield of $\mathbb{F}_{p^k}^\times$, $x^{\frac{p^k-1}{r}} = 1$.

- When k is even, say $\mathbb{F}_{p^k} = \mathbb{F}_{p^{k/2}}(u)$.
  $E(\mathbb{F}_{p^k})[r] \simeq E'(\mathbb{F}_{p^{k/2}})[r] \Longrightarrow P = (x, yu)$ with $x, y \in \mathbb{F}_{p^{k/2}}$.
  Vertical lines $v_S(P) \in \mathbb{F}_{p^{k/2}}$
- When $4 \mid k$ and $b = 0$ or $6 \mid k$ and $a = 0$, line computations are more efficient

$$f = \left(1^2 \cdot \ell_{Q,Q}(P)\right)^2 \cdot \ell_{2Q,2Q}(P) \cdot \ell_{4Q,Q}(P)$$

The final exponentiation is $(f_{t-1,Q}(P))^{\frac{p^k-1}{r}}$

Proposition

For x in a subfield of $\mathbb{F}_{p^k}^{\times}$, $x^{\frac{p^k-1}{r}} = 1$.

- When k is even, say $\mathbb{F}_{p^k} = \mathbb{F}_{p^{k/2}}(u)$.
  $E(\mathbb{F}_{p^k})[r] \simeq E'(\mathbb{F}_{p^{k/2}})[r] \Longrightarrow P = (x, yu)$ with $x, y \in \mathbb{F}_{p^{k/2}}$.
  Vertical lines $v_S(P) \in \mathbb{F}_{p^{k/2}}$
- When $4 \mid k$ and $b = 0$ or $6 \mid k$ and $a = 0$, line computations are more efficient

$$f = \left(1^2 \cdot \ell_{Q,Q}(P)\right)^2 \cdot \ell_{2Q,2Q}(P) \cdot \ell_{4Q,Q}(P)$$

The final exponentiation is $(f_{t-1,Q}(P))^{\frac{p^k-1}{r}}$

Proposition

For x in a subfield of $\mathbb{F}_{p^k}^{\times}$, $x^{\frac{p^k-1}{r}} = 1$.

- When k is even, say $\mathbb{F}_{p^k} = \mathbb{F}_{p^{k/2}}(u)$.
  $E(\mathbb{F}_{p^k})[r] \simeq E'(\mathbb{F}_{p^{k/2}})[r] \Longrightarrow P = (x, yu)$ with $x, y \in \mathbb{F}_{p^{k/2}}$.
  Vertical lines $v_S(P) \in \mathbb{F}_{p^{k/2}}$
- When $4 \mid k$ and $b = 0$ or $6 \mid k$ and $a = 0$, line computations are more efficient

$$f = \ell_{Q,Q}(P)^2 \ell_{2Q,2Q}(P) \ell_{4Q,Q}(P)$$

Final exponentiation.

Final exponentiation.

$$x^{\frac{p^k-1}{r}}$$

Final exponentiation.

$$x^{\frac{p^k-1}{r}}$$

$$\frac{p^k-1}{r} = \frac{p^k-1}{\Phi_k(p)}\frac{\Phi_k(p)}{r}$$

Final exponentiation.

$$x^{\frac{p^k-1}{r}}$$

$$\frac{p^k-1}{r} = \frac{p^k-1}{\Phi_k(p)} \frac{\Phi_k(p)}{r}$$

$\frac{p^k-1}{\Phi_k(p)}$ is a polynomial in p. Easy exponentiation with Frobenius.

Final exponentiation.

$$x^{\frac{p^k-1}{r}}$$

$$\frac{p^k-1}{r} = \frac{p^k-1}{\Phi_k(p)}\frac{\Phi_k(p)}{r}$$

$\frac{p^k-1}{\Phi_k(p)}$ is a polynomial in p. Easy exponentiation with Frobenius.

Last part $\frac{\Phi_k(p)}{r}$: more expensive, decompose into polynomials and compute efficiently with Horner rule.

Pairing-friendly curves for 128 bits of security

An elliptic curve E defined over $\mathbb{F}_p$, of trace t and discriminant D is pairing-friendly of embedding degree k if

- p, r are primes and t is relatively prime to p
- r divides $p+1-t$ and p^k-1 but does not divide p^i-1 for $1 \leq i < k$
- $4p-t^2 = Dy^2$ for a sufficiently small positive integer D and an integer y.

An elliptic curve E defined over $\mathbb{F}_p$, of trace t and discriminant D is pairing-friendly of embedding degree k if

- p, r are primes and t is relatively prime to p
- r divides $p+1-t$ and p^k-1 but does not divide p^i-1 for $1 \leq i < k$
- $4p - t^2 = Dy^2$ for a sufficiently small positive integer D and an integer y.

Example.

Barreto-Naehrig curves are elliptic curves of embedding degree $k = 12$, parametrized by

$$p(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$$

$$r(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$$

$$t(x) = 6x^2 + 1$$

For some integer x_0, $(p(x_0), r(x_0), t(x_0))$ parametrizes a pairing-friendly elliptic curve.

Miller loop.

k is even $\Longrightarrow$ no vertical lines.

$6 \mid k$ and $D = 3 \Longrightarrow$ twist of order 6: $E(\mathbb{F}_{p^{12}})[r] \simeq E'(\mathbb{F}_{p^2})[r]$.

Miller loop.

k is even $\implies$ no vertical lines.

$6 \mid k$ and $D = 3 \implies$ twist of order 6: $E(\mathbb{F}_{p^{12}})[r] \simeq E'(\mathbb{F}_{p^2})[r]$.

Final exponentiation.

$$\frac{p^{12}-1}{r} = (p^6-1)(p^2+1)\frac{p^4-p^2+1}{r}$$

Miller loop.
k is even $\implies$ no vertical lines.
$6 \mid k$ and $D = 3 \implies$ twist of order 6: $E(\mathbb{F}_{p^{12}})[r] \simeq E'(\mathbb{F}_{p^2})[r]$.
Final exponentiation.

$$\frac{p^{12}-1}{r} = (p^6-1)(p^2+1)\frac{p^4-p^2+1}{r}$$

$y = (x^{p^6-1})^{p^2+1}$ is easy with Frobenius powers.

Miller loop.

k is even $\Longrightarrow$ no vertical lines.

$6 \mid k$ and $D = 3 \Longrightarrow$ twist of order 6: $E(\mathbb{F}_{p^{12}})[r] \simeq E'(\mathbb{F}_{p^2})[r]$.

Final exponentiation.

$$\frac{p^{12}-1}{r} = (p^6-1)(p^2+1)\frac{p^4-p^2+1}{r}$$

$y = (x^{p^6-1})^{p^2+1}$ is easy with Frobenius powers.

$\frac{p^4-p^2+1}{r}$ is specific because $p = p(x_0)$ and $r = r(x_0)$.

Miller loop.
k is even $\Longrightarrow$ no vertical lines.
$6 \mid k$ and $D = 3 \Longrightarrow$ twist of order 6: $E(\mathbb{F}_{p^{12}})[r] \simeq E'(\mathbb{F}_{p^2})[r]$.
Final exponentiation.

$$\frac{p^{12}-1}{r} = (p^6-1)(p^2+1)\frac{p^4-p^2+1}{r}$$

$y = (x^{p^6-1})^{p^2+1}$ is easy with Frobenius powers.
$\frac{p^4-p^2+1}{r}$ is specific because $p = p(x_0)$ and $r = r(x_0)$.
$y^{\frac{p(x_0)^4-p(x_0)^2+1}{r(x_0)}} = y^{\alpha(x_0)}$ with α polynomial: few exponentiations to x_0.

Miller loop.

k is even $\Longrightarrow$ no vertical lines.

$6 \mid k$ and $D = 3 \Longrightarrow$ twist of order 6: $E(\mathbb{F}_{p^{12}})[r] \simeq E'(\mathbb{F}_{p^2})[r]$.

Final exponentiation.

$$\frac{p^{12}-1}{r} = (p^6-1)(p^2+1)\frac{p^4-p^2+1}{r}$$

$y = (x^{p^6-1})^{p^2+1}$ is easy with Frobenius powers.

$\frac{p^4-p^2+1}{r}$ is specific because $p = p(x_0)$ and $r = r(x_0)$.

$y^{\frac{p(x_0)^4-p(x_0)^2+1}{r(x_0)}} = y^{\alpha(x_0)}$ with α polynomial: few exponentiations to x_0.

Efficient pairing.  But how secure are these curves ?

Security of pairing curves.

$$e : E(\mathbb{F}_p) \times E(\mathbb{F}_{p^k}) \longrightarrow \mathbb{F}_{p^k}$$

Security of pairing curves.

$$e : E(\mathbb{F}_p) \times E(\mathbb{F}_{p^k}) \longrightarrow \mathbb{F}_{p^k}$$

- Security against DHP in elliptic curve: best attack in $\mathcal{O}(\sqrt{r})$.

Security of pairing curves.

$$e : E(\mathbb{F}_p) \times E(\mathbb{F}_{p^k}) \longrightarrow \mathbb{F}_{p^k}$$

- Security against DHP in elliptic curve: best attack in $\mathcal{O}(\sqrt{r})$.
- Security against DHP in $\mathbb{F}_{p^k}$: Number Field Sieve attacks in progress.

special prime p	$\Longrightarrow$ 1993: Special NFS attack
$k > 1$	$\Longrightarrow$ 2015: Tower NFS attack
composite k and special p	$\Longrightarrow$ 2016: STNFS attack

Security of pairing curves.

$$e : E(\mathbb{F}_p) \times E(\mathbb{F}_{p^k}) \longrightarrow \mathbb{F}_{p^k}$$

- Security against DHP in elliptic curve: best attack in $\mathcal{O}(\sqrt{r})$.
- Security against DHP in $\mathbb{F}_{p^k}$: Number Field Sieve attacks in progress.

special prime p	$\Longrightarrow$	1993: Special NFS attack
$k > 1$	$\Longrightarrow$	2015: Tower NFS attack
composite k and special p	$\Longrightarrow$	2016: STNFS attack

BN curves are threatened by STNFS... 
Need a 5500 bits field $\mathbb{F}_{p^{12}}$ to get 128 bits of security.

Generation of curves with given prime k, square-free D and no structure on p.

Algorithm: $\textsc{Cocks-Pinch}(k, D)$ – Compute a pairing-friendly curve $E/\mathbb{F}_p$ of trace t with a subgroup of order r, such that $t^2 - Dy^2 = 4p$.

Set a prime r such that $k \mid r - 1$ and $\sqrt{-D} \in \mathbb{F}_r$
Set T such that $r \mid \Phi_k(T)$
$t \leftarrow T + 1$
$y \leftarrow (t - 2)/\sqrt{-D}$
Lift $t, y \in \mathbb{Z}$ such that $t^2 + Dy^2 \equiv 0 \mod 4$
$p \leftarrow (t^2 + Dy^2)/4$
if p is prime **then return** $[p, t, y, r]$ **else** Repeat with another r.

Generation of curves with given prime k, square-free D and no structure on p.

Algorithm: $\textsc{Cocks-Pinch}(k, D)$ – Compute a pairing-friendly curve $E/\mathbb{F}_p$ of trace t with a subgroup of order r, such that $t^2 - Dy^2 = 4p$.

Set a prime r such that $k \mid r-1$ and $\sqrt{-D} \in \mathbb{F}_r$
Set T such that $r \mid \Phi_k(T)$
$t \leftarrow T + 1$
$y \leftarrow (t-2)/\sqrt{-D}$
Lift $t, y \in \mathbb{Z}$ such that $t^2 + Dy^2 \equiv 0 \mod 4$
$p \leftarrow (t^2 + Dy^2)/4$
if p is prime **then return** $[p, t, y, r]$ **else** Repeat with another r.

Large trace $t \implies$ the ate pairing is not very efficient 

Generation of curves with given prime k, square-free D and no structure on p.

Algorithm: $\textsc{Cocks-Pinch}(k, D)$ – Compute a pairing-friendly curve $E/\mathbb{F}_p$ of trace t with a subgroup of order r, such that $t^2 - Dy^2 = 4p$.

Set a small T
Set a prime r such that $k \mid r - 1$, $\sqrt{-D} \in \mathbb{F}_r$ and $r \mid \Phi_k(T)$
$t \leftarrow T + 1$
$y \leftarrow (t - 2)/\sqrt{-D}$
Lift $t, y \in \mathbb{Z}$ such that $t^2 + Dy^2 \equiv 0 \mod 4$
$p \leftarrow (t^2 + Dy^2)/4$
if p is prime **then return** $[p, t, y, r]$ **else** Repeat with another r.

Large trace $t \implies$ the ate pairing is not very efficient 

Fix: first fix a small T and then choose r. $t = T + 1$ is small 

Generation of curves with given prime k, square-free D and no structure on p.

Algorithm: $\textsc{Cocks-Pinch}(k, D)$ – Compute a pairing-friendly curve $E/\mathbb{F}_p$ of trace t with a subgroup of order r, such that $t^2 - Dy^2 = 4p$.

Set a small T
Set a prime r such that $k \mid r - 1$, $\sqrt{-D} \in \mathbb{F}_r$ and $r \mid \varphi_k(T)$
$t \leftarrow T + 1$
$y \leftarrow (t-2)/\sqrt{-D}$
Lift $t, y \in \mathbb{Z}$ such that $t^2 + Dy^2 \equiv 0 \mod 4$
$p \leftarrow (t^2 + Dy^2)/4$
if p is prime **then return** $[p, t, y, r]$ **else** Repeat with another r.

Large trace $t \implies$ the ate pairing is not very efficient

Fix: first fix a small T and then choose r. $t = T + 1$ is small
$f_{T,Q}(P)^{(p^k-1)/r}$ is also a pairing [Hess 2009].

Generation of curves with given prime k, square-free D and no structure on p.

Algorithm: $\textsc{Cocks-Pinch}(k, D)$ – Compute a pairing-friendly curve $E/\mathbb{F}_p$ of trace t with a subgroup of order r, such that $t^2 - Dy^2 = 4p$.

Set a small T
Set a prime r such that $k \mid r-1$, $\sqrt{-D} \in \mathbb{F}_r$ and $r \mid \varphi_k(T)$
$t \leftarrow T + 1$
$y \leftarrow (t-2)/\sqrt{-D}$
Lift $t, y \in \mathbb{Z}$ such that $t^2 + Dy^2 \equiv 0 \mod 4$
$p \leftarrow (t^2 + Dy^2)/4$
if p is prime and $p = 1 \bmod k$ **then return** $[p, t, y, r]$ **else** Repeat with another r.

Large trace $t \implies$ the ate pairing is not very efficient

Fix: first fix a small T and then choose r. $t = T + 1$ is small

$f_{T,Q}(P)^{(p^k-1)/r}$ is also a pairing [Hess 2009]. $\mathbb{F}_{p^k} = \mathbb{F}_p[u]/(u^k - \alpha)$

128-bit security for finite field extensions.

128-bit security for finite field extensions.

Our variant of Cocks-Pinch generates pairing-friendly curves with a "non-special" prime p.

128-bit security for finite field extensions.

Our variant of Cocks-Pinch generates pairing-friendly curves with a "non-special" prime p.

Field	DL attack	Field size needed for 128-bit security	$\log_2(p)$ induced
$\mathbb{F}_{p^5}$	TNFS	3320	664
$\mathbb{F}_{p^6}$	exTNFS	4032	672
$\mathbb{F}_{p^7}$	TNFS	3584	512
$\mathbb{F}_{p^8}$	exTNFS	4352	544

Timings and comparisons

New curves for 128 bits of security.

We generate curves of embedding degree $5, 6, 7$ and 8 with the previous algorithm.

Curve	this work				BN	BLS	–
k	5	6	7	8	12	12	1
$\mathbb{F}_{p^k}$ *size*	3320	4032	3584	4352	5544	5532	3072
$\log_2(p)$	664	672	512	544	462	461	3072
$\mathbb{F}_p$ mul.	230ns	230ns	130ns	154ns	130ns	130ns	4882ns
Miller length	64-bit	128-bit	43-bit	64-bit	117-bit	77-bit	256-bit
Mill. field	3320	672	3584	1088	924	922	3072
Miller step	3.4ms	1.1ms	2.1ms	0.7ms	1.6ms	1.0ms	22.7ms
Expo. step	2.5ms	0.9ms	1.9ms	1.0ms	0.7ms	0.8ms	20.0ms
Total	5.9ms	2.0ms	4.0ms	1.7ms	2.3ms	1.8ms	42.7ms

New curves for 128 bits of security.

We generate curves of embedding degree $5, 6, 7$ and 8 with the previous algorithm.

Curve	this work				BN	BLS	–
k	5	6	7	8	12	12	1
$\mathbb{F}_{p^k}$ *size*	3320	4032	3584	4352	5544	5532	3072
$\log_2(p)$	664	672	512	544	462	461	3072
$\mathbb{F}_p$ mul.	230ns	230ns	130ns	154ns	130ns	130ns	4882ns
Miller length	64-bit	128-bit	43-bit	64-bit	117-bit	77-bit	256-bit
Mill. field	3320	672	3584	1088	924	922	3072
Miller step	3.4ms	1.1ms	2.1ms	0.7ms	1.6ms	1.0ms	22.7ms
Expo. step	2.5ms	0.9ms	1.9ms	1.0ms	0.7ms	0.8ms	20.0ms
Total	5.9ms	2.0ms	4.0ms	1.7ms	2.3ms	1.8ms	42.7ms

New curves for 128 bits of security.

We generate curves of embedding degree $5, 6, 7$ and 8 with the previous algorithm.

Curve	this work				BN	BLS	–
k	5	6	7	8	12	12	1
$\mathbb{F}_{p^k}$ *size*	3320	4032	3584	4352	5544	5532	3072
$\log_2(p)$	664	672	512	544	462	461	3072
$\mathbb{F}_p$ mul.	230ns	230ns	130ns	154ns	130ns	130ns	4882ns
Miller length	64-bit	128-bit	43-bit	64-bit	117-bit	77-bit	256-bit
Mill. field	3320	672	3584	1088	924	922	3072
Miller step	3.4ms	1.1ms	2.1ms	0.7ms	1.6ms	1.0ms	22.7ms
Expo. step	2.5ms	0.9ms	1.9ms	1.0ms	0.7ms	0.8ms	20.0ms
Total	5.9ms	2.0ms	4.0ms	1.7ms	2.3ms	1.8ms	42.7ms

New curves for 128 bits of security.

We generate curves of embedding degree $5, 6, 7$ and 8 with the previous algorithm.

Curve	this work				BN	BLS	–
k	5	6	7	8	12	12	1
$\mathbb{F}_{p^k}$ *size*	3320	4032	3584	4352	5544	5532	3072
$\log_2(p)$	664	672	512	544	462	461	3072
$\mathbb{F}_p$ mul.	230ns	230ns	130ns	154ns	130ns	130ns	4882ns
Miller length	64-bit	128-bit	43-bit	64-bit	117-bit	77-bit	256-bit
Mill. field	3320	672	3584	1088	924	922	3072
Miller step	3.4ms	1.1ms	2.1ms	0.7ms	1.6ms	1.0ms	22.7ms
Expo. step	2.5ms	0.9ms	1.9ms	1.0ms	0.7ms	0.8ms	20.0ms
Total	5.9ms	2.0ms	4.0ms	1.7ms	2.3ms	1.8ms	42.7ms

New curves for 128 bits of security.

We generate curves of embedding degree $5, 6, 7$ and 8 with the previous algorithm.

Curve	this work				BN	BLS	–
k	5	6	7	8	12	12	1
$\mathbb{F}_{p^k}$ *size*	3320	4032	3584	4352	5544	5532	3072
$\log_2(p)$	664	672	512	544	462	461	3072
$\mathbb{F}_p$ mul.	230ns	230ns	130ns	154ns	130ns	130ns	4882ns
Miller length	64-bit	128-bit	43-bit	64-bit	117-bit	77-bit	256-bit
Mill. field	3320	672	3584	1088	924	922	3072
Miller step	3.4ms	1.1ms	2.1ms	0.7ms	1.6ms	1.0ms	22.7ms
Expo. step	2.5ms	0.9ms	1.9ms	1.0ms	0.7ms	0.8ms	20.0ms
Total	5.9ms	2.0ms	4.0ms	1.7ms	2.3ms	1.8ms	42.7ms

New curves for 128 bits of security.

We generate curves of embedding degree $5, 6, 7$ and 8 with the previous algorithm.

Curve	this work				BN	BLS	–
k	5	6	7	8	12	12	1
$\mathbb{F}_{p^k}$ *size*	3320	4032	3584	4352	5544	5532	3072
$\log_2(p)$	664	672	512	544	462	461	3072
$\mathbb{F}_p$ mul.	230ns	230ns	130ns	154ns	130ns	130ns	4882ns
Miller length	64-bit	128-bit	43-bit	64-bit	117-bit	77-bit	256-bit
Mill. field	3320	672	3584	1088	924	922	3072
Miller step	3.4ms	1.1ms	2.1ms	0.7ms	1.6ms	1.0ms	22.7ms
Expo. step	2.5ms	0.9ms	1.9ms	1.0ms	0.7ms	0.8ms	20.0ms
Total	5.9ms	2.0ms	4.0ms	1.7ms	2.3ms	1.8ms	42.7ms

New curves for 128 bits of security.

We generate curves of embedding degree $5, 6, 7$ and 8 with the previous algorithm.

Curve	this work				BN	BLS	–
k	5	6	7	8	12	12	1
$\mathbb{F}_{p^k}$ *size*	3320	4032	3584	4352	5544	5532	3072
$\log_2(p)$	664	672	512	544	462	461	3072
$\mathbb{F}_p$ mul.	230ns	230ns	130ns	154ns	130ns	130ns	4882ns
Miller length	64-bit	128-bit	43-bit	64-bit	117-bit	77-bit	256-bit
Mill. field	3320	672	3584	1088	924	922	3072
Miller step	3.4ms	1.1ms	2.1ms	0.7ms	1.6ms	1.0ms	22.7ms
Expo. step	2.5ms	0.9ms	1.9ms	1.0ms	0.7ms	0.8ms	20.0ms
Total	5.9ms	2.0ms	4.0ms	1.7ms	2.3ms	1.8ms	42.7ms

New curves for 128 bits of security.

We generate curves of embedding degree $5, 6, 7$ and 8 with the previous algorithm.

Curve	this work				BN	BLS	–
k	5	6	7	8	12	12	1
$\mathbb{F}_{p^k}$ *size*	3320	4032	3584	4352	5544	5532	3072
$\log_2(p)$	664	672	512	544	462	461	3072
$\mathbb{F}_p$ mul.	230ns	230ns	130ns	154ns	130ns	130ns	4882ns
Miller length	64-bit	128-bit	43-bit	64-bit	117-bit	77-bit	256-bit
Mill. field	3320	672	3584	1088	924	922	3072
Miller step	3.4ms	1.1ms	2.1ms	0.7ms	1.6ms	1.0ms	22.7ms
Expo. step	2.5ms	0.9ms	1.9ms	1.0ms	0.7ms	0.8ms	20.0ms
Total	5.9ms	2.0ms	4.0ms	1.7ms	2.3ms	1.8ms	42.7ms

Thank you for your attention.

Thank you for your attention.

Thank you for your attention.

Thank you for your attention.

Thank you for your attention.

Thank you for your attention.

Thank you for your attention.

Curve	this work				BN	BLS	KSS	–
k	5	6	7	8	12	12	16	1
$\mathbb{F}_{p^k}$ *size*	3320	4032	3584	4352	5544	5532	5424	3072
$\log_2(p)$	664	672	512	544	462	461	339	3072
$\mathbb{F}_p$ mul.	230ns	230ns	130ns	154ns	130ns	130ns	69ns	4882ns
Miller length	64-bit	128-bit	43-bit	64-bit	117-bit	77-bit	35-bit	256-bit
Mill. field	3320	672	3584	1088	924	922	1356	3072
Miller step	3.4ms	1.1ms	2.1ms	0.7ms	1.6ms	1.0ms	0.5ms	22.7ms
Expo. step	2.5ms	0.9ms	1.9ms	1.0ms	0.7ms	0.8ms	1.3ms	20.0ms
Total	5.9ms	2.0ms	4.0ms	1.7ms	2.3ms	1.8ms	1.8ms	42.7ms