Public-key Compression for SIKE

Michael Naehrig   Joost Renes

Microsoft Research   Radboud University

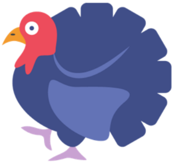
10 December 2019

Post-Quantum Cryptography

(generic post-quantum crypto intro...)

Ostrich — Turkey

CECPQ2 = HRSS + X25519

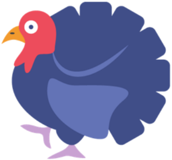


CECPQ2b = SIKE + X25519

https://blog.cloudflare.com/the-tls-post-quantum-experiment/

Ostrich — Turkey — Chicken

CECPQ2 = HRSS + X25519



CECPQ2b = SIKE + X25519

CECPQ2c = SIKEc + X25519

https://blog.cloudflare.com/the-tls-post-quantum-experiment/

Isogenies: Rational Maps between Elliptic Curves

$\mathbb{Z}$

Polynomial

Described by **coefficients**

$$f(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_n x^n = \sum_{i=0}^{n} c_i x^i$$

$\mathbb{Z}$

Isogenies: Rational Maps between Elliptic Curves

$\mathbb{Z}$

Polynomial

Described by **roots**

$$f(x) = c \cdot \prod_{i=0}^{n} (x - a_i)$$

$\mathbb{Z}$

Isogenies: Rational Maps between Elliptic Curves

$\mathbb{Q}$

Rational map

Described by **roots** of f and g

$$f(x)/g(x) = \prod_{i=0}^{n}(x - a_i) / \prod_{i=0}^{n}(x - b_i)$$

$\mathbb{Q}$

Isogenies: Rational Maps between Elliptic Curves

$\overline{\mathbb{F}}_p$

Rational map

Described by **roots** of f and g

$$f(x)/g(x) = \prod_{i=0}^{n}(x - a_i) / \prod_{i=0}^{n}(x - b_i)$$

$\overline{\mathbb{F}}_p$

Isogenies: Rational Maps between Elliptic Curves

$$\overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p$$

Rational map

$$\Big(f(x,y)/g(x,y), h(x,y)/k(x,y) \Big)$$

$$\downarrow$$

$$\overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p$$

Isogenies: Rational Maps between Elliptic Curves

$$\{ (x, y) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p \mid y^2 = x^3 + A \cdot x^2 + x \} \cup \{\infty\}$$

Rational map

$$\Big(f(x,y)/g(x,y), h(x,y)/k(x,y) \Big)$$

$$\downarrow$$

$$\{ (x, y) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p \mid y^2 = x^3 + \overline{A} \cdot x^2 + x \} \cup \{\infty\}$$

Isogenies: Rational Maps between Elliptic Curves

$$\{\ (x,y) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p \mid y^2 = x^3 + A \cdot x^2 + x\ \} \cup \{\infty\}$$

Isogeny $(\infty \mapsto \infty)$

$$\Big(f(x)/g(x), y \cdot h(x)/k(x) \Big)$$

$$\{\ (x,y) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p \mid y^2 = x^3 + \overline{A} \cdot x^2 + x\ \} \cup \{\infty\}$$

Isogenies: Rational Maps between Elliptic Curves

$$\{\,(x,y) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p \mid y^2 = x^3 + A \cdot x^2 + x\,\} \cup \{\infty\}$$

Isogeny ($\infty \mapsto \infty$)

Described by **roots** of **g**

$$\left(f(x)/g(x), y \cdot h(x)/k(x) \right)$$

$$\{\,(x,y) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p \mid y^2 = x^3 + \overline{A} \cdot x^2 + x\,\} \cup \{\infty\}$$

Isogenies: Rational Maps between Elliptic Curves

$$\{\ (x,y) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p \mid y^2 = x^3 + A \cdot x^2 + x\ \} \cup \{\infty\}$$

Isogeny ($\infty \mapsto \infty$)

Described by **roots** of **g**

$$\Big(f(x)/g(x), y \cdot h(x)/k(x) \Big)$$

Isogeny degree $\sim \#\,\mathrm{roots}(g)$

$\sim \deg(g)$

$$\{\ (x,y) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p \mid y^2 = x^3 + \overline{A} \cdot x^2 + x\ \} \cup \{\infty\}$$

Isogenies: Rational Maps between Elliptic Curves

$$\{\ (x,y) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p \mid y^2 = x^3 + A \cdot x^2 + x\ \} \cup \{\infty\}$$

Isogeny $(\infty \mapsto \infty)$

Described by **roots** of **g**

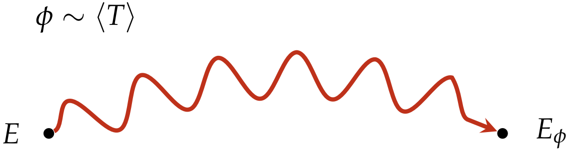
$$\left(f(x)/g(x), y \cdot h(x)/k(x) \right)$$

Cyclic isogeny
when $\ker(g) = \langle T \rangle$

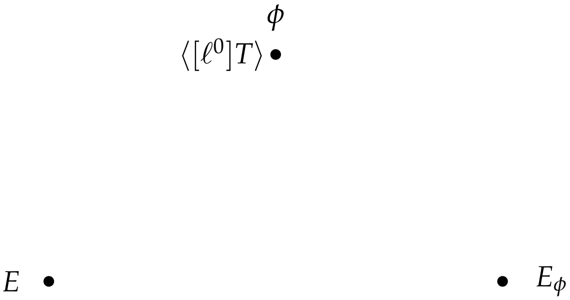
Isogeny degree $\sim \#\,\mathrm{roots}(g)$
$\sim \deg(g)$

$$\{\ (x,y) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p \mid y^2 = x^3 + \overline{A} \cdot x^2 + x\ \} \cup \{\infty\}$$

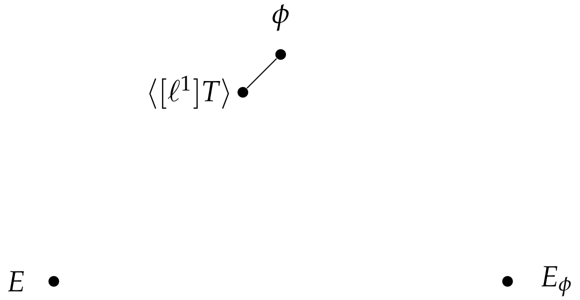
Compression and Dual Isogenies



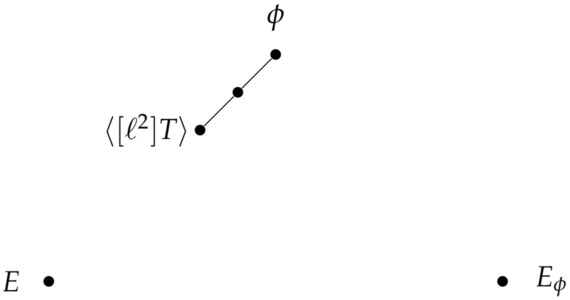
Compression and Dual Isogenies



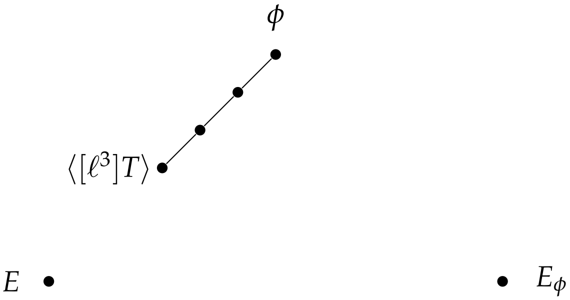
Compression and Dual Isogenies



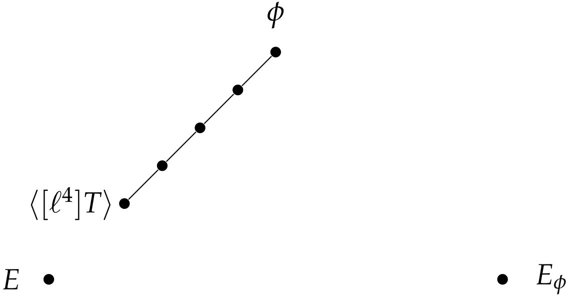
Compression and Dual Isogenies



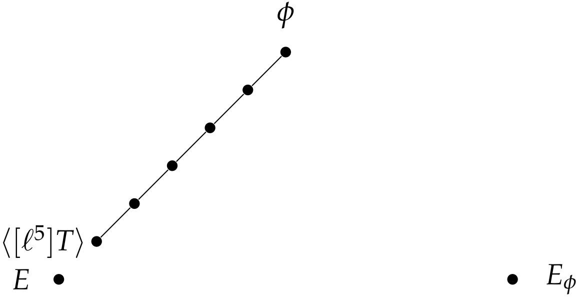
Compression and Dual Isogenies



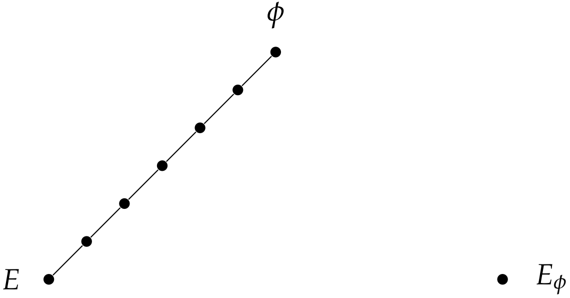
Compression and Dual Isogenies



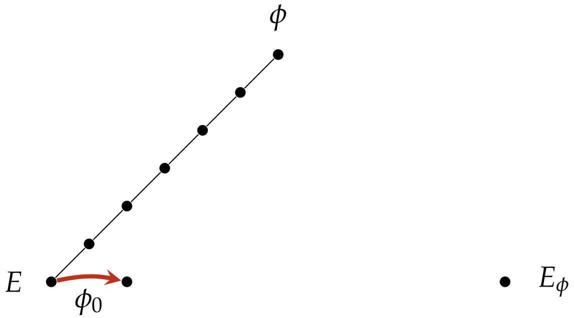
Compression and Dual Isogenies



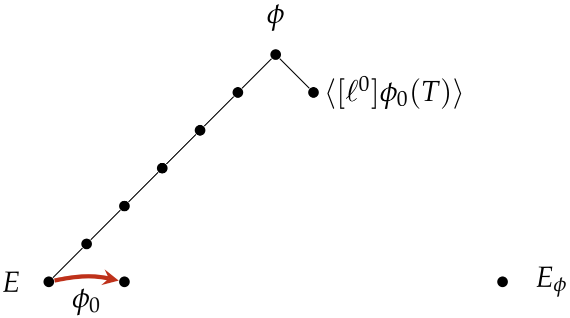
Compression and Dual Isogenies



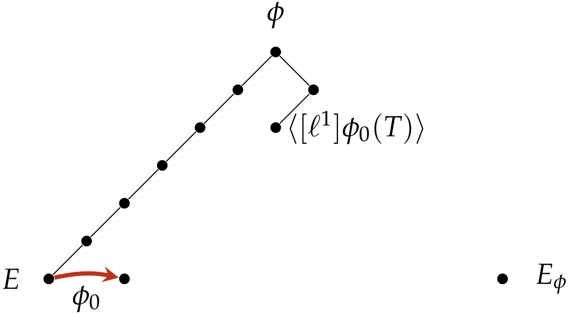
Compression and Dual Isogenies



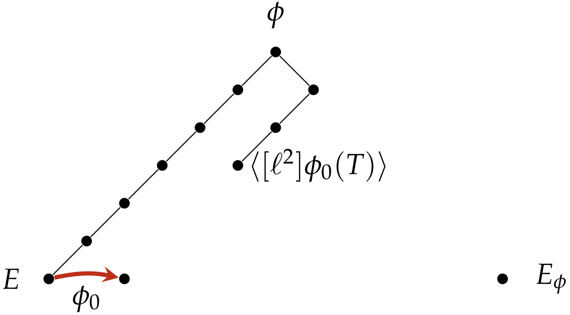
Compression and Dual Isogenies



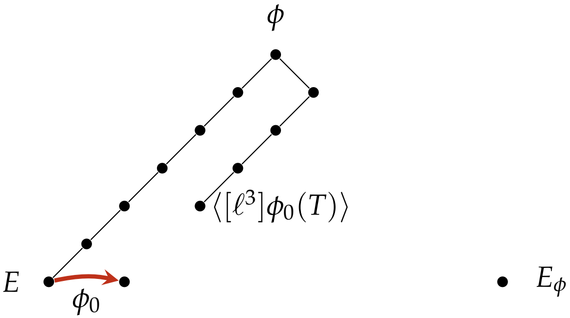
Compression and Dual Isogenies



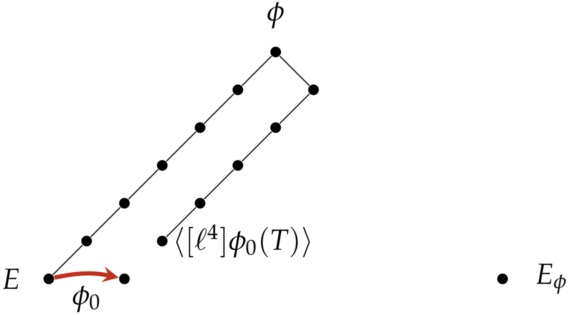
Compression and Dual Isogenies



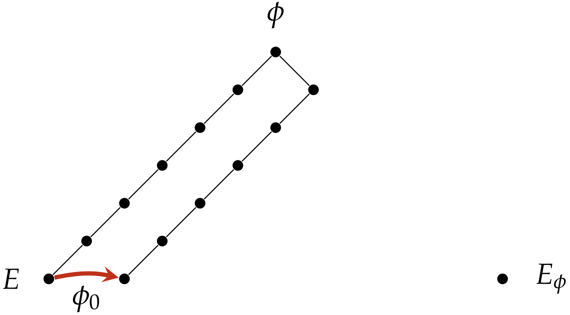
Compression and Dual Isogenies



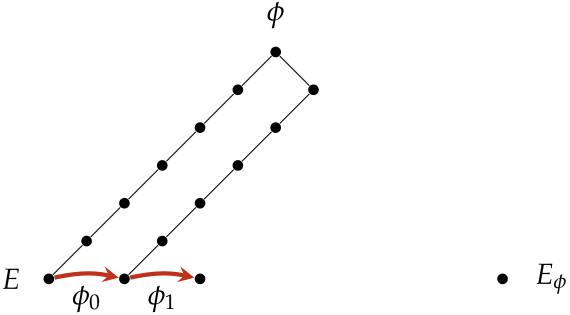
Compression and Dual Isogenies



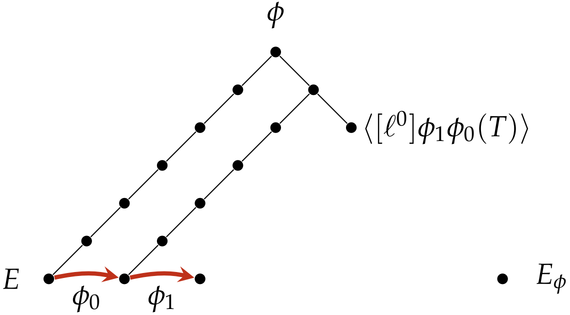
Compression and Dual Isogenies



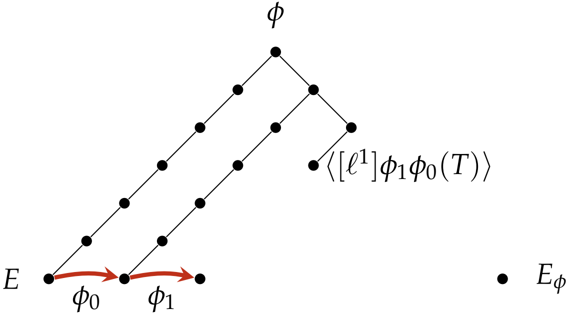
Compression and Dual Isogenies



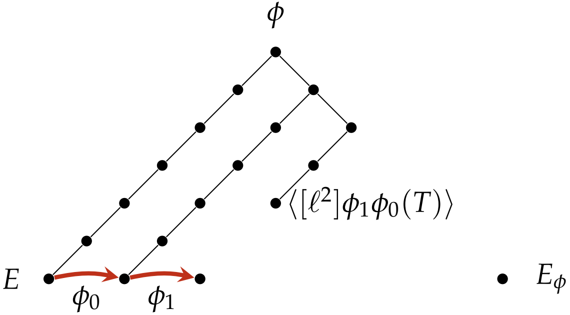
Compression and Dual Isogenies



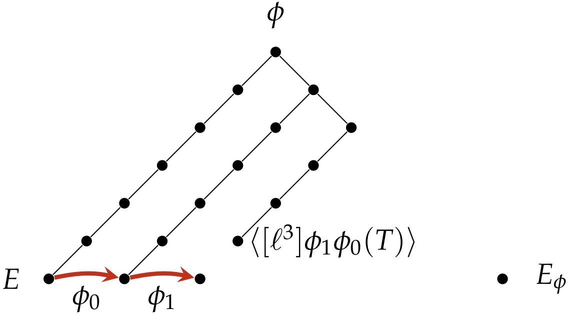
Compression and Dual Isogenies



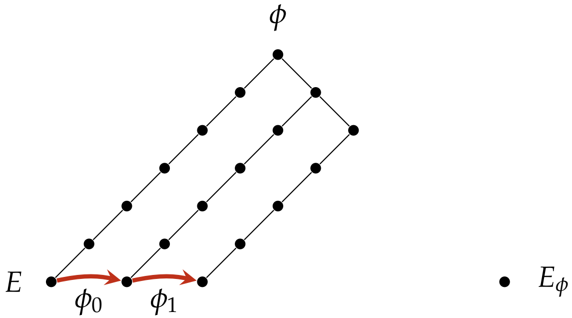
Compression and Dual Isogenies



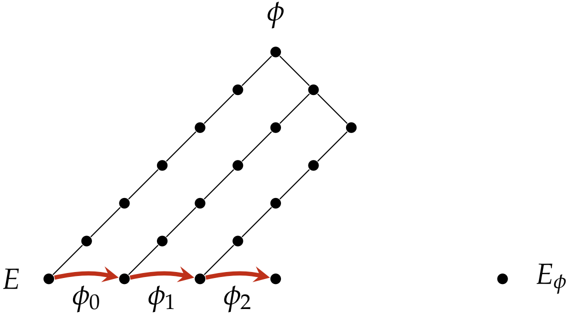
Compression and Dual Isogenies



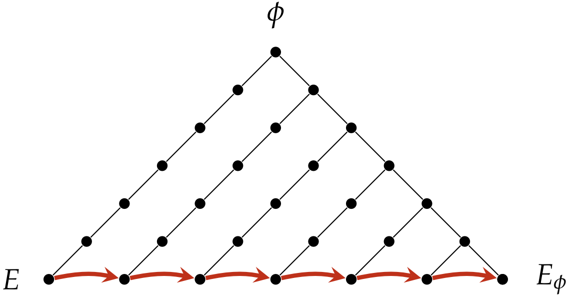
Compression and Dual Isogenies



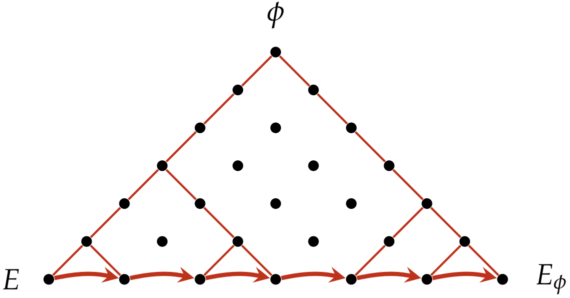
Compression and Dual Isogenies



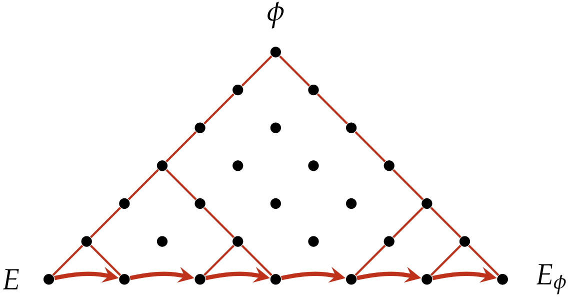
Compression and Dual Isogenies



Compression and Dual Isogenies

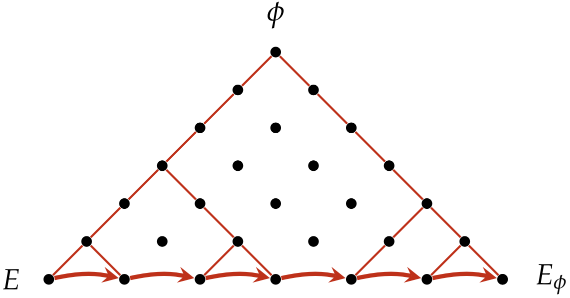


Compression and Dual Isogenies



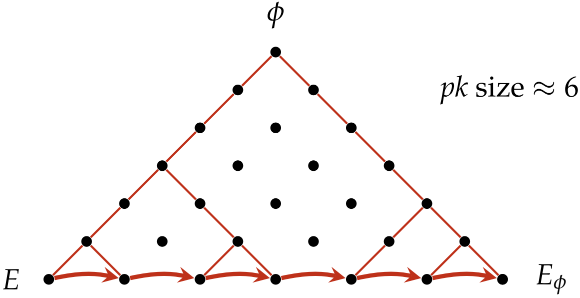
$$\begin{pmatrix} P \\ Q \end{pmatrix}$$

Compression and Dual Isogenies



$$\begin{pmatrix} P \\ Q \end{pmatrix} \qquad \begin{pmatrix} \phi(P) \\ \phi(Q) \end{pmatrix}$$

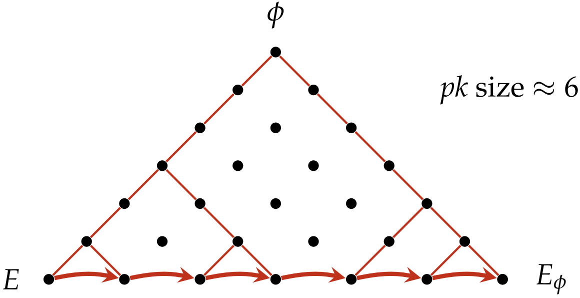
Compression and Dual Isogenies



pk size $\approx 6 \log p$

$$\begin{pmatrix} P \\ Q \end{pmatrix} \qquad \begin{pmatrix} \phi(P) \\ \phi(Q) \end{pmatrix}$$

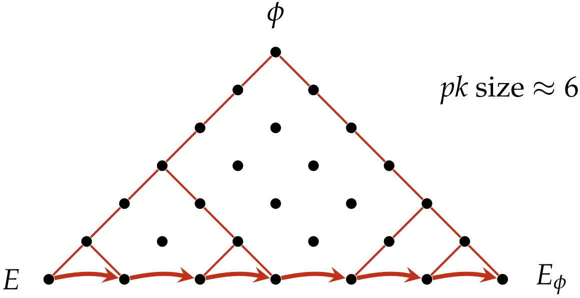
Compression and Dual Isogenies



pk size $\approx 6 \log p$

$$\begin{pmatrix} P \\ Q \end{pmatrix} \qquad \begin{pmatrix} \phi(P) \\ \phi(Q) \end{pmatrix} \qquad \begin{pmatrix} R \\ S \end{pmatrix}$$

Compression and Dual Isogenies

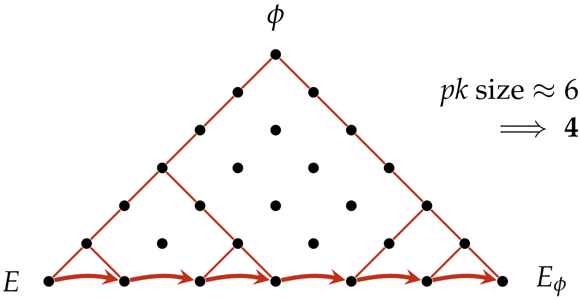


pk size $\approx 6 \log p$

$$\begin{pmatrix} P \\ Q \end{pmatrix}$$

$$\begin{pmatrix} \phi(P) \\ \phi(Q) \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} R \\ S \end{pmatrix}$$

Compression and Dual Isogenies

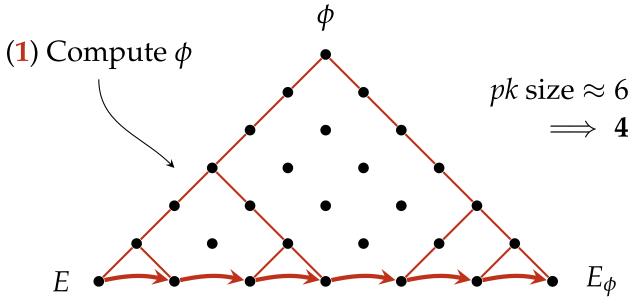


pk size $\approx 6 \log p$
$\implies$ $\mathbf{4} \log p$

$$\begin{pmatrix} P \\ Q \end{pmatrix}$$

$$\begin{pmatrix} \phi(P) \\ \phi(Q) \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} R \\ S \end{pmatrix}$$

Compression and Dual Isogenies



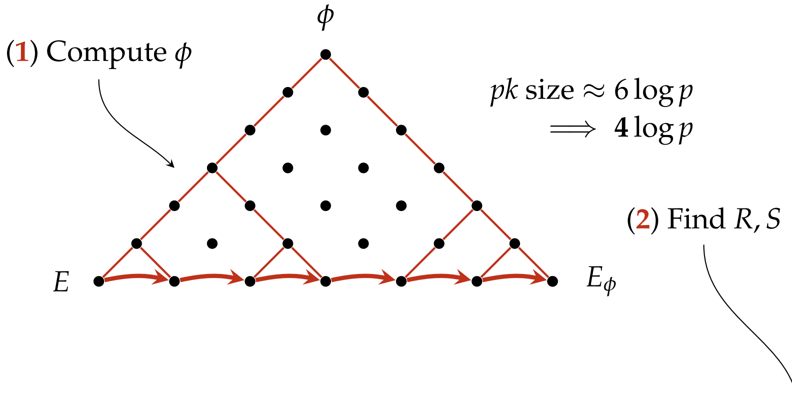
pk size $\approx 6 \log p$

$\implies$ $\mathbf{4} \log p$

$$\begin{pmatrix} P \\ Q \end{pmatrix}$$

$$\begin{pmatrix} \phi(P) \\ \phi(Q) \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} R \\ S \end{pmatrix}$$

Compression and Dual Isogenies



pk size $\approx 6 \log p$

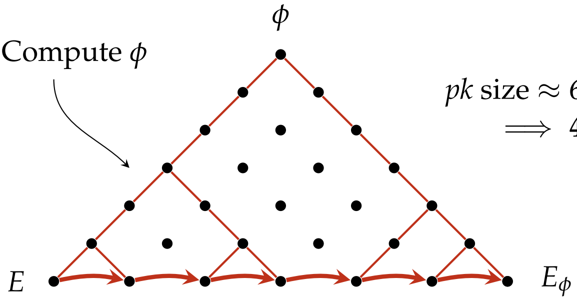
$\implies \mathbf{4} \log p$

$$\begin{pmatrix} P \\ Q \end{pmatrix}$$

$$\begin{pmatrix} \phi(P) \\ \phi(Q) \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} R \\ S \end{pmatrix}$$

Compression and Dual Isogenies

(**1**) Compute ϕ



pk size $\approx 6 \log p$

$\implies$ **4** $\log p$

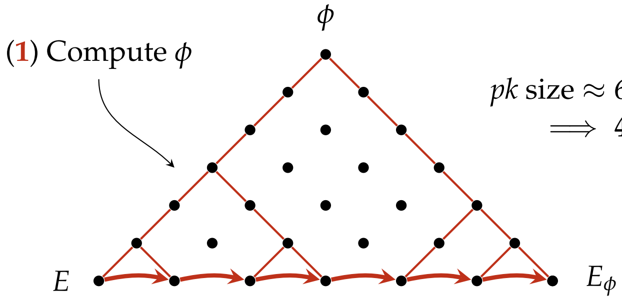
(**2**) Find R, S

(**3**) Compute $\phi(P), \phi(Q)$

$$\begin{pmatrix} P \\ Q \end{pmatrix}$$

$$\begin{pmatrix} \phi(P) \\ \phi(Q) \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} R \\ S \end{pmatrix}$$

Compression and Dual Isogenies



pk size $\approx 6 \log p$

$\implies \mathbf{4} \log p$

(**2**) Find R, S

(**3**) Compute $\phi(P), \phi(Q)$

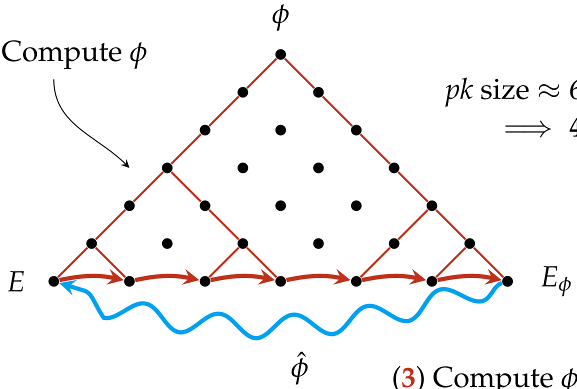
$$\begin{pmatrix} P \\ Q \end{pmatrix}$$

$$\begin{pmatrix} \phi(P) \\ \phi(Q) \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} R \\ S \end{pmatrix}$$

(**4**) Find $\alpha, \beta, \gamma, \delta$

Compression and Dual Isogenies

(**1**) Compute ϕ



pk size $\approx 6\log p$

$\implies \mathbf{4}\log p$

(**2**) Find R, S

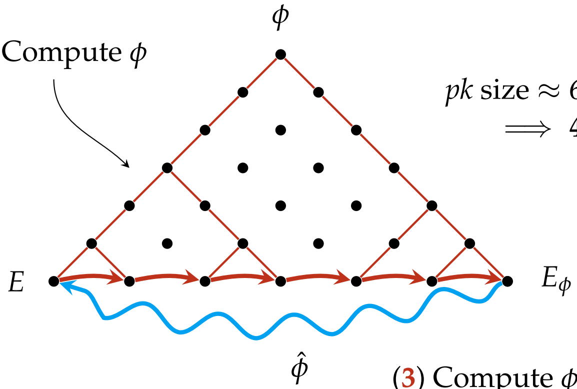
(**3**) Compute $\phi(P), \phi(Q)$

$$\begin{pmatrix} P \\ Q \end{pmatrix} \qquad \begin{pmatrix} \phi(P) \\ \phi(Q) \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} R \\ S \end{pmatrix}$$

(**4**) Find $\alpha, \beta, \gamma, \delta$

Compression and Dual Isogenies

(**1**) Compute ϕ



pk size $\approx 6 \log p$

$\implies$ $\mathbf{4} \log p$

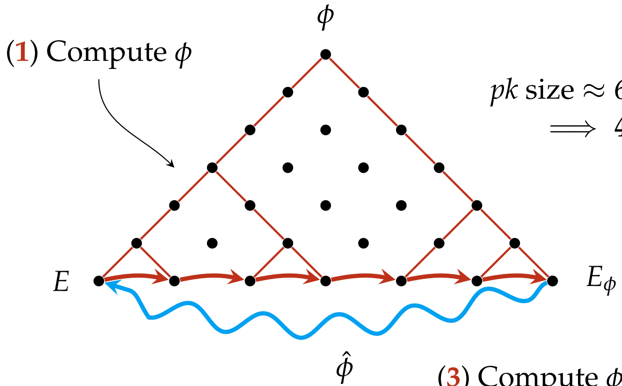
(**2**) Find R, S

(**3**) Compute $\phi(P), \phi(Q)$

$$\begin{pmatrix} P \\ Q \end{pmatrix} \qquad \begin{pmatrix} \hat{\phi}(R) \\ \hat{\phi}(S) \end{pmatrix} \qquad \begin{pmatrix} \phi(P) \\ \phi(Q) \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} R \\ S \end{pmatrix}$$

(**4**) Find $\alpha, \beta, \gamma, \delta$

Compression and Dual Isogenies



pk size $\approx 6 \log p$

$\implies$ **4** $\log p$

(2) Find R, S

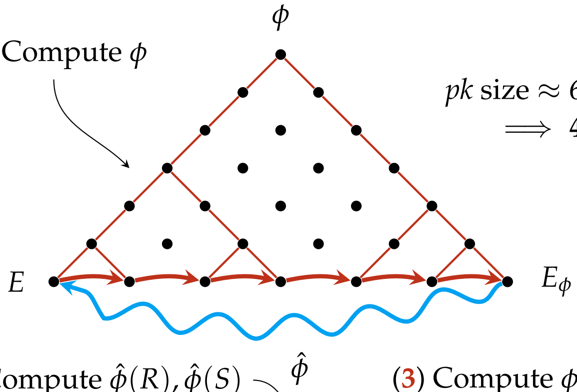
(3) Compute $\phi(P), \phi(Q)$

$$\begin{pmatrix} P \\ Q \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \hat{\phi}(R) \\ \hat{\phi}(S) \end{pmatrix} \qquad \begin{pmatrix} \phi(P) \\ \phi(Q) \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} R \\ S \end{pmatrix}$$

(4) Find $\alpha, \beta, \gamma, \delta$

Compression and Dual Isogenies

(**1**) Compute ϕ



pk size $\approx 6\log p$
$\implies \mathbf{4}\log p$

(**2**) Find R, S

(**3**) Compute $\hat{\phi}(R), \hat{\phi}(S)$

$$\begin{pmatrix} P \\ Q \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \hat{\phi}(R) \\ \hat{\phi}(S) \end{pmatrix}$$

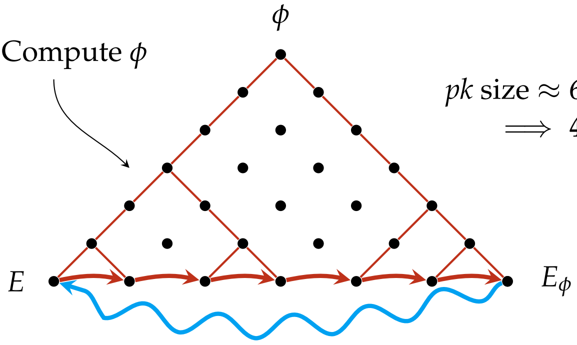
(**3**) Compute $\phi(P), \phi(Q)$

$$\begin{pmatrix} \phi(P) \\ \phi(Q) \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} R \\ S \end{pmatrix}$$

(**4**) Find $\alpha, \beta, \gamma, \delta$

Compression and Dual Isogenies

(**1**) Compute ϕ



pk size $\approx 6 \log p$
$\implies$ **4** $\log p$

(**2**) Find R, S

$\hat{\phi}$

(**3**) Compute $\hat{\phi}(R), \hat{\phi}(S)$

$$\begin{pmatrix} P \\ Q \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \hat{\phi}(R) \\ \hat{\phi}(S) \end{pmatrix}$$

(**4**) Find $\alpha, \beta, \gamma, \delta$

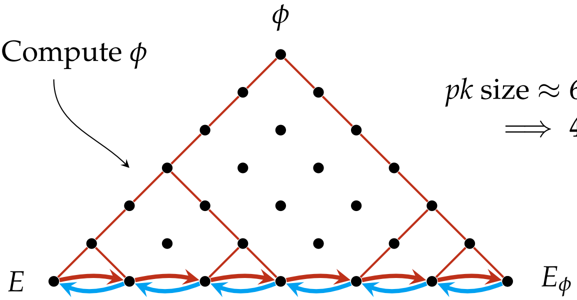
(**3**) Compute $\phi(P), \phi(Q)$

$$\begin{pmatrix} \phi(P) \\ \phi(Q) \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} R \\ S \end{pmatrix}$$

(**4**) Find $\alpha, \beta, \gamma, \delta$

Compression and Dual Isogenies

(**1**) Compute ϕ



pk size $\approx 6 \log p$

$\implies \mathbf{4} \log p$

(**2**) Find R, S

(**3**) Compute $\hat{\phi}(R), \hat{\phi}(S)$

$$\begin{pmatrix} P \\ Q \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \hat{\phi}(R) \\ \hat{\phi}(S) \end{pmatrix}$$

(**4**) Find $\alpha, \beta, \gamma, \delta$

(**3**) Compute $\phi(P), \phi(Q)$

$$\begin{pmatrix} \phi(P) \\ \phi(Q) \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} R \\ S \end{pmatrix}$$

(**4**) Find $\alpha, \beta, \gamma, \delta$

Speedups/slowdowns for (1) – (3)

	ℓ	p434	p503	p610	p751
SIKE-2	2	9 649	13 332	24 238	35 294
This	2	**7 921**	**11 039**	**20 269**	**30 922**
SIKE-2	3	7 062	9 859	16 830	28 258
This	3	**7 368**	**10 211**	**17 497**	**29 397**

Table 1: Efficiency for isogeny + basis gen. in 10^3 cycles on Skylake.

Supersingular Isogeny Key Encapsulation – `https://sike.org`.

(4) Find $\alpha, \beta, \gamma, \delta$

$$\begin{pmatrix} P \\ Q \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} \hat{\phi}(R) \\ \hat{\phi}(S) \end{pmatrix}$$

(4) Find $\alpha, \beta, \gamma, \delta$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} P \\ Q \end{pmatrix} = \qquad \begin{pmatrix} \hat{\phi}(R) \\ \hat{\phi}(S) \end{pmatrix}$$

(4) Find $\alpha, \beta, \gamma, \delta$

$$[a]P + [b]Q = \hat{\phi}(R)$$
$$[c]P + [d]Q = \hat{\phi}(S)$$

(4) Find $\alpha, \beta, \gamma, \delta$

$$[a]P + [b]Q = \hat{\phi}(R)$$
$$[c]P + [d]Q = \hat{\phi}(S)$$

$$\begin{aligned}
\tau(Q, \hat{\phi}(R)) &= \tau(P, Q)^{-a} \\
\tau(P, \hat{\phi}(R)) &= \tau(P, Q)^{b} \\
\tau(Q, \hat{\phi}(S)) &= \tau(P, Q)^{-c} \\
\tau(P, \hat{\phi}(S)) &= \tau(P, Q)^{d}
\end{aligned}$$

(4) Find $\alpha, \beta, \gamma, \delta$

$$[a]P + [b]Q = \hat{\phi}(R)$$
$$[c]P + [d]Q = \hat{\phi}(S)$$

$$\begin{aligned}
\tau(Q, \hat{\phi}(R)) &= \tau(P, Q)^{-a} \\
\tau(P, \hat{\phi}(R)) &= \tau(P, Q)^{b} \\
\tau(Q, \hat{\phi}(S)) &= \tau(P, Q)^{-c} \\
\tau(P, \hat{\phi}(S)) &= \tau(P, Q)^{d}
\end{aligned}$$

(reduced) **Tate** pairing

(4) Find $\alpha, \beta, \gamma, \delta$

$$[a]P + [b]Q = \hat{\phi}(R)$$
$$[c]P + [d]Q = \hat{\phi}(S)$$

$$\begin{aligned} \tau(Q, \hat{\phi}(R)) &= \tau(P, Q)^{-a} \\ \tau(P, \hat{\phi}(R)) &= \tau(P, Q)^{b} \\ \tau(Q, \hat{\phi}(S)) &= \tau(P, Q)^{-c} \\ \tau(P, \hat{\phi}(S)) &= \tau(P, Q)^{d} \end{aligned}$$

(reduced) **Tate** pairing

(4) Quadruple Tate pairing

Output: $\tau(P, \hat{\phi}(R))$

$f \leftarrow 1$

for $i = 1$ **to** e **do**

  $f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(R))$

end for

(4) Quadruple Tate pairing

Output: $\tau(P, \hat{\phi}(R))$

$f \leftarrow 1$

for $i = 1$ **to** e **do**

  $f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(R))$

end for

(4) Quadruple Tate pairing

Output: $\tau(P, \hat{\phi}(R))$
$f \leftarrow 1$
for $i = 1$ **to** e **do**
$f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(R))$
end for

$g_{[2]P}$

(4) Quadruple Tate pairing

Output: $\tau(P, \hat{\phi}(R))$
  $f \leftarrow 1$
  for $i = 1$ **to** e **do**
    $f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(R))$
  end for

$g_{[2]P}$
$g_{[4]P}$

(4) Quadruple Tate pairing

Output: $\tau(P, \hat{\phi}(R))$

$f \leftarrow 1$

for $i = 1$ **to** e **do**

$f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(R))$

end for

$g_{[2]P}$

$g_{[4]P}$

$g_{[8]P}$

(4) Quadruple Tate pairing

Output: $\tau(P, \hat{\phi}(R))$
  $f \leftarrow 1$
  for $i = 1$ **to** e **do**
    $f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(R))$
  end for

$\longrightarrow$

$g_{[2]P}$
$g_{[4]P}$
$g_{[8]P}$
$g_{[16]P}$

(4) Quadruple Tate pairing

Output: $\tau(P, \hat{\phi}(R))$
$f \leftarrow 1$
for $i = 1$ **to** e **do**
$f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(R))$
end for

$g_{[2]P}$
$g_{[4]P}$
$g_{[8]P}$
$g_{[16]P}$
$\vdots$

(4) Quadruple Tate pairing

Output: $\tau(P, \hat{\phi}(R))$
$f \leftarrow 1$
for $i = 1$ **to** e **do**
$f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(R))$
end for

Output: $\tau(P, \hat{\phi}(S))$
$f \leftarrow 1$
for $i = 1$ **to** e **do**
$f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(S))$
end for

$g_{[2]P}$
$g_{[4]P}$
$g_{[8]P}$
$g_{[16]P}$
$\vdots$

(4) Quadruple Tate pairing

Output: $\tau(P, \hat{\phi}(R))$
$f \leftarrow 1$
for $i = 1$ **to** e **do**
$f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(R))$
end for

Output: $\tau(P, \hat{\phi}(S))$
$f \leftarrow 1$
for $i = 1$ **to** e **do**
$f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(S))$
end for

$g_{[2]P}$
$g_{[4]P}$
$g_{[8]P}$
$g_{[16]P}$
$\vdots$

(4) Quadruple Tate pairing

Output: $\tau(P, \hat{\phi}(R))$
$f \leftarrow 1$
for $i = 1$ **to** e **do**
$f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(R))$
end for

Output: $\tau(P, \hat{\phi}(S))$
$f \leftarrow 1$
for $i = 1$ **to** e **do**
$f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(S))$
end for

$g_{[2]P}$
$g_{[4]P}$
$g_{[8]P}$
$g_{[16]P}$
$\vdots$

(4) Quadruple Tate pairing

Output: $\tau(P, \hat{\phi}(R))$
  $f \leftarrow 1$
  for $i = 1$ **to** e **do**
    $f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(R))$
  end for

Output: $\tau(P, \hat{\phi}(S))$
  $f \leftarrow 1$
  for $i = 1$ **to** e **do**
    $f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(S))$
  end for

$g_{[2]P}$
$g_{[4]P}$
$g_{[8]P}$
$g_{[16]P}$
$\vdots$

(4) Quadruple Tate pairing

Output: $\tau(P, \hat{\phi}(R))$
  $f \leftarrow 1$
  for $i = 1$ **to** e **do**
    $f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(R))$
  end for

Output: $\tau(P, \hat{\phi}(S))$
  $f \leftarrow 1$
  for $i = 1$ **to** e **do**
    $f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(S))$
  end for

$g_{[2]P}$
$g_{[4]P}$
$g_{[8]P}$
$g_{[16]P}$
$\vdots$

(4) Quadruple Tate pairing

Output: $\tau(P, \hat{\phi}(R))$
$f \leftarrow 1$
for $i = 1$ **to** e **do**
$f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(R))$
end for

Output: $\tau(P, \hat{\phi}(S))$
$f \leftarrow 1$
for $i = 1$ **to** e **do**
$f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(S))$
end for

$g_{[2]P}$
$g_{[4]P}$
$g_{[8]P}$
$g_{[16]P}$
$\vdots$

(4) Quadruple Tate pairing

Output: $\tau(P, \hat{\phi}(R))$
$f \leftarrow 1$
for $i = 1$ **to** e **do**
$f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(R))$
end for

Output: $\tau(P, \hat{\phi}(S))$
$f \leftarrow 1$
for $i = 1$ **to** e **do**
$f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(S))$
end for

$g_{[2]P}$
$g_{[4]P}$
$g_{[8]P}$
$g_{[16]P}$
$\vdots$

(a) Store table of $g_{[2^i]P}$

(4) Quadruple Tate pairing

Output: $\tau(P, \hat{\phi}(R))$
$f \leftarrow 1$
for $i = 1$ **to** e **do**
$f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(R))$
end for

Output: $\tau(P, \hat{\phi}(S))$
$f \leftarrow 1$
for $i = 1$ **to** e **do**
$f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(S))$
end for

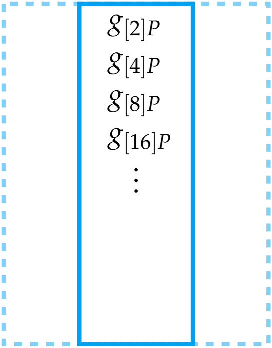
$g_{[2]P}$
$g_{[4]P}$
$g_{[8]P}$
$g_{[16]P}$
$\vdots$

(a) Store table of $g_{[2^i]P}$
(b) $P = (x, y)$ in $\mathbb{F}_p \times \mathbb{F}_p$

(4) Quadruple Tate pairing

Output: $\tau(P, \hat{\phi}(R))$
  $f \leftarrow 1$
  for $i = 1$ **to** e **do**
    $f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(R))$
  end for

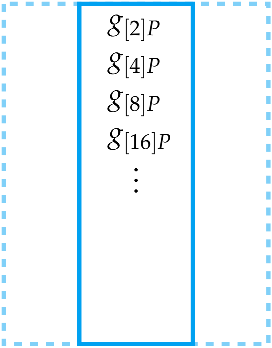
Output: $\tau(P, \hat{\phi}(S))$
  $f \leftarrow 1$
  for $i = 1$ **to** e **do**
    $f \leftarrow f^2 \cdot g_{[2^i]P}(\hat{\phi}(S))$
  end for



(a) Store table of $g_{[2^i]P}$
(b) $P = (x, y)$ in $\mathbb{F}_p \times \mathbb{F}_p$

(4) Quadruple Tate pairing

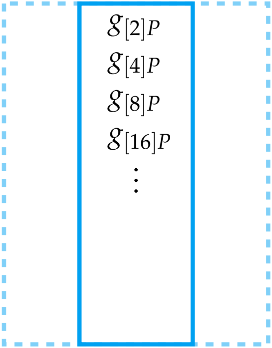
Output: $\tau(Q, \hat{\phi}(R))$
$f \leftarrow 1$
for $i = 1$ **to** e **do**
$f \leftarrow f^2 \cdot g_{[2^i]Q}(\hat{\phi}(R))$
end for



(a) Store table of $g_{[2^i]P}$
(b) $P = (x, y)$ in $\mathbb{F}_p \times \mathbb{F}_p$

(4) Quadruple Tate pairing

Output: $\tau(Q, \hat{\phi}(R))$
  $f \leftarrow 1$
  for $i = 1$ **to** e **do**
    $f \leftarrow f^2 \cdot g_{[2^i]Q}(\hat{\phi}(R))$
  end for



(a) Store table of $g_{[2^i]P}$
(b) $P = (x, y)$ in $\mathbb{F}_p \times \mathbb{F}_p$

(4) Quadruple Tate pairing

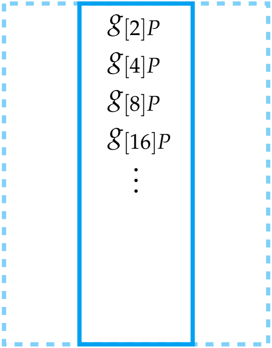
Output: $\tau(Q, \hat{\phi}(R))$

$f \leftarrow 1$

for $i = 1$ **to** e **do**

$\quad f \leftarrow f^2 \cdot g_{\psi([2^i]P)}(\hat{\phi}(R))$

end for



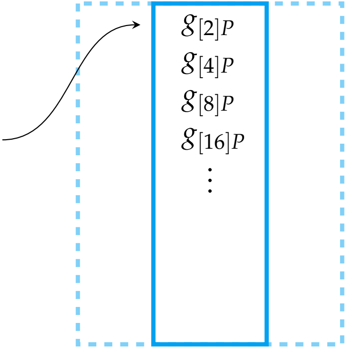
(a) Store table of $g_{[2^i]P}$

(b) $P = (x, y)$ in $\mathbb{F}_p \times \mathbb{F}_p$

(c) $Q = \psi(P) = (-x, iy)$

(4) Quadruple Tate pairing

Output: $\tau(Q, \hat{\phi}(R))$
  $f \leftarrow 1$
  for $i = 1$ **to** e **do**
    $f \leftarrow f^2 \cdot g_{\psi([2^i]P)}(\hat{\phi}(R))$
  end for



(a) Store table of $g_{[2^i]P}$
(b) $P = (x, y)$ in $\mathbb{F}_p \times \mathbb{F}_p$
(c) $Q = \psi(P) = (-x, iy)$

(4) Quadruple Tate pairing

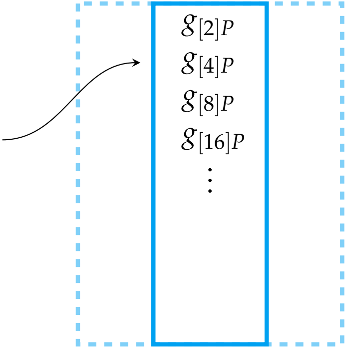
Output: $\tau(Q, \hat{\phi}(R))$

$f \leftarrow 1$

for $i = 1$ **to** e **do**

  $f \leftarrow f^2 \cdot g_{\psi([2^i]P)}(\hat{\phi}(R))$

end for



(a) Store table of $g_{[2^i]P}$

(b) $P = (x, y)$ in $\mathbb{F}_p \times \mathbb{F}_p$

(c) $Q = \psi(P) = (-x, iy)$

(4) Quadruple Tate pairing

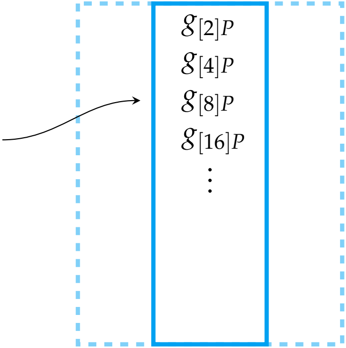
Output: $\tau(Q, \hat{\phi}(R))$

$f \leftarrow 1$

for $i = 1$ **to** e **do**

$f \leftarrow f^2 \cdot g_{\psi([2^i]P)}(\hat{\phi}(R))$

end for



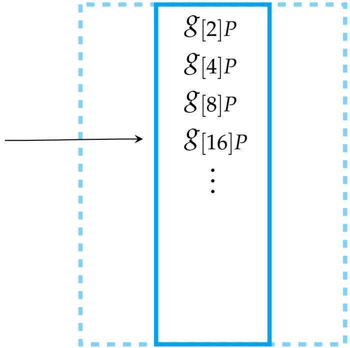
(a) Store table of $g_{[2^i]P}$

(b) $P = (x, y)$ in $\mathbb{F}_p \times \mathbb{F}_p$

(c) $Q = \psi(P) = (-x, iy)$

(4) Quadruple Tate pairing

Output: $\tau(Q, \hat{\phi}(R))$
  $f \leftarrow 1$
  for $i = 1$ **to** e **do**
    $f \leftarrow f^2 \cdot g_{\psi([2^i]P)}(\hat{\phi}(R))$
  end for

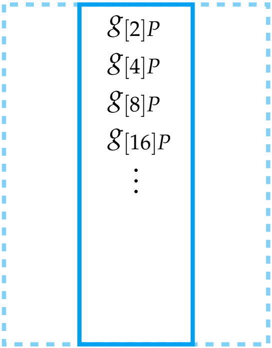


(a) Store table of $g_{[2^i]P}$
(b) $P = (x, y)$ in $\mathbb{F}_p \times \mathbb{F}_p$
(c) $Q = \psi(P) = (-x, iy)$

(4) Quadruple Tate pairing

Output: $\tau(Q, \hat{\phi}(R))$
  $f \leftarrow 1$
  for $i = 1$ **to** e **do**
    $f \leftarrow f^2 \cdot g_{\psi([2^i]P)}(\hat{\phi}(R))$
  end for

Output: $\tau(Q, \hat{\phi}(S))$
  $f \leftarrow 1$
  for $i = 1$ **to** e **do**
    $f \leftarrow f^2 \cdot g_{\psi([2^i]P)}(\hat{\phi}(S))$
  end for

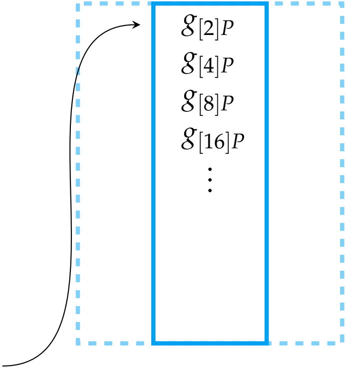


(a) Store table of $g_{[2^i]P}$
(b) $P = (x, y)$ in $\mathbb{F}_p \times \mathbb{F}_p$
(c) $Q = \psi(P) = (-x, iy)$

(4) Quadruple Tate pairing

Output: $\tau(Q, \hat{\phi}(R))$
  $f \leftarrow 1$
  for $i = 1$ **to** e **do**
    $f \leftarrow f^2 \cdot g_{\psi([2^i]P)}(\hat{\phi}(R))$
  end for

Output: $\tau(Q, \hat{\phi}(S))$
  $f \leftarrow 1$
  for $i = 1$ **to** e **do**
    $f \leftarrow f^2 \cdot g_{\psi([2^i]P)}(\hat{\phi}(S))$
  end for

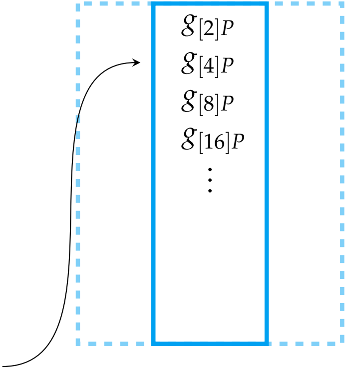


(a) Store table of $g_{[2^i]P}$
(b) $P = (x, y)$ in $\mathbb{F}_p \times \mathbb{F}_p$
(c) $Q = \psi(P) = (-x, iy)$

(4) Quadruple Tate pairing

Output: $\tau(Q, \hat{\phi}(R))$
$f \leftarrow 1$
for $i = 1$ **to** e **do**
$f \leftarrow f^2 \cdot g_{\psi([2^i]P)}(\hat{\phi}(R))$
end for

Output: $\tau(Q, \hat{\phi}(S))$
$f \leftarrow 1$
for $i = 1$ **to** e **do**
$f \leftarrow f^2 \cdot g_{\psi([2^i]P)}(\hat{\phi}(S))$
end for

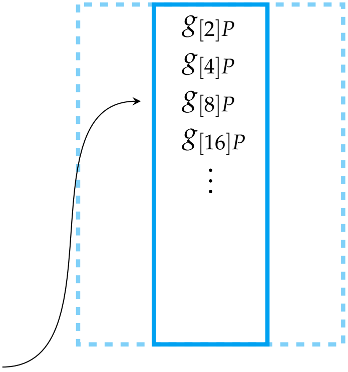


(a) Store table of $g_{[2^i]P}$
(b) $P = (x, y)$ in $\mathbb{F}_p \times \mathbb{F}_p$
(c) $Q = \psi(P) = (-x, iy)$

(4) Quadruple Tate pairing

Output: $\tau(Q, \hat{\phi}(R))$
$f \leftarrow 1$
for $i = 1$ **to** e **do**
$f \leftarrow f^2 \cdot g_{\psi([2^i]P)}(\hat{\phi}(R))$
end for

Output: $\tau(Q, \hat{\phi}(S))$
$f \leftarrow 1$
for $i = 1$ **to** e **do**
$f \leftarrow f^2 \cdot g_{\psi([2^i]P)}(\hat{\phi}(S))$
end for

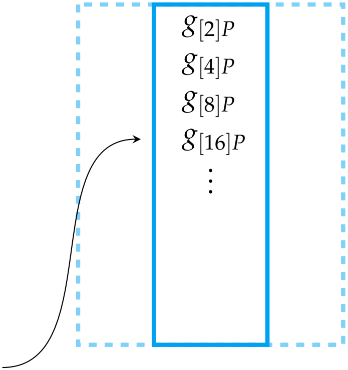


(a) Store table of $g_{[2^i]P}$
(b) $P = (x, y)$ in $\mathbb{F}_p \times \mathbb{F}_p$
(c) $Q = \psi(P) = (-x, iy)$

(4) Quadruple Tate pairing

Output: $\tau(Q, \hat{\phi}(R))$
  $f \leftarrow 1$
  for $i = 1$ **to** e **do**
    $f \leftarrow f^2 \cdot g_{\psi([2^i]P)}(\hat{\phi}(R))$
  end for

Output: $\tau(Q, \hat{\phi}(S))$
  $f \leftarrow 1$
  for $i = 1$ **to** e **do**
    $f \leftarrow f^2 \cdot g_{\psi([2^i]P)}(\hat{\phi}(S))$
  end for



(a) Store table of $g_{[2^i]P}$
(b) $P = (x, y)$ in $\mathbb{F}_p \times \mathbb{F}_p$
(c) $Q = \psi(P) = (-x, iy)$

Speedups for (4)

	ℓ	p434	p503	p610	p751
SIKE-2	2	5 821	8 033	13 458	21 908
This		**1 954**	**2 676**	**4 525**	**7 348**
SIKE-2	3	4 921	6 716	11 365	18 224
This		**1 821**	**2 486**	**4 214**	**6 727**

Table 2: Efficiency of pairing in 10^3 cycles on Skylake.

Supersingular Isogeny Key Encapsulation – `https://sike.org`.

Speedups for SIKE

	pk	KeyGen	Encaps	Decaps
SIKE-2	330 B	6 482	10 563	11 290
SIKE-2-comp	196 B	16 397	20 056	18 622
This	196 B	**10 849**	**16 600**	**15 682**

Table 3: Efficiency of KEM in 10^3 cycles on Skylake for `p434`.

Supersingular Isogeny Key Encapsulation – `https://sike.org`.

Speedups for SIKE

	pk	KeyGen	Encaps	Decaps
SIKE-2	—	—	—	—
SIKE-2-comp	−41%	153%	90%	65%
This	−41%	**67%**	**57%**	**39%**

Table 3: Efficiency of KEM in percentage on Skylake for `p434`.

Supersingular Isogeny Key Encapsulation – `https://sike.org`.

Thanks for your atthention!