

# SQIPrime: A dimension 2 variant of SQISignHD with non-smooth challenge isogenies

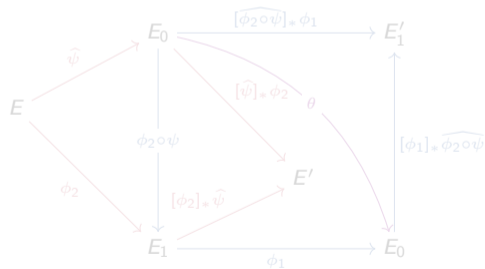
Max DUPARC & Tako Boris FOUOTSA



Asiacrypt 2024: Kolkata

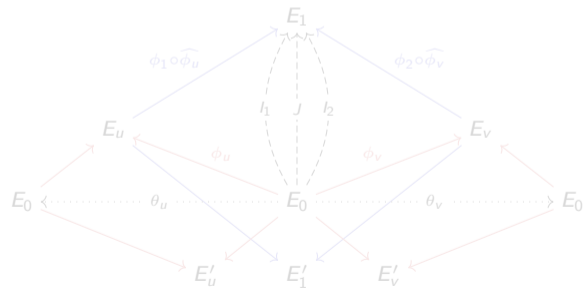
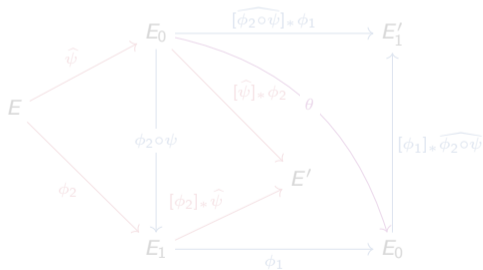
# SQIPrime

- SQIPrime does SQIsign2D using:
  - Non-smooth challenge isogenies.
  - Kani's Lemma.
  - Diagrams.



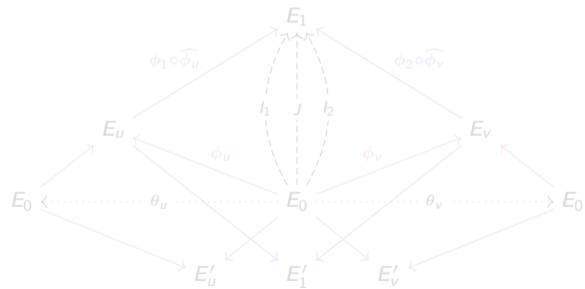
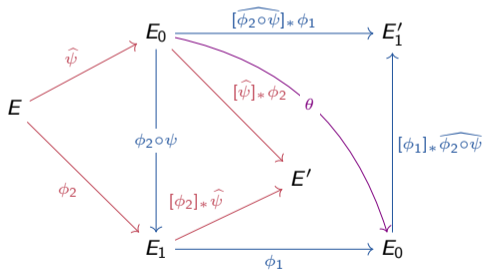
# SQIPrime

- SQIPrime does SQIsign2D using:
  - Non-smooth challenge isogenies.
  - Kani's Lemma.
  - Diagrams.



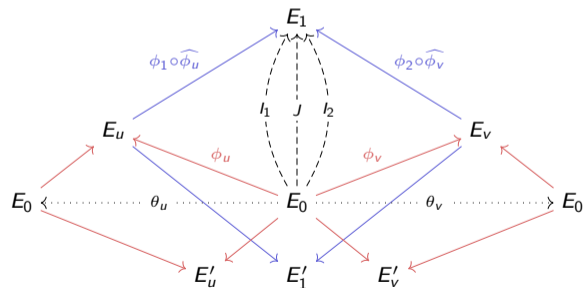
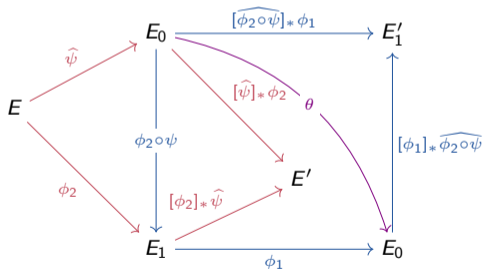
# SQIPrime

- SQIPrime does SQIsign2D using:
  - Non-smooth challenge isogenies.
  - Kani's Lemma.
  - Diagrams.



# SQIPrime

- SQIPrime does SQIsign2D using:
  - Non-smooth challenge isogenies.
  - Kani's Lemma.
  - Diagrams.



# DeuringVRF Basis

- Finding  $I_\phi$  is easy if  $\deg(\phi)$  smooth, but what if  $\deg(\phi)$  non-smooth ?

## DeuringVRF Basis

A **DeuringVRF basis**  $(P, Q, \iota, I_P)$  is:

- $P, Q \in E$  such that  $\langle P, Q \rangle = E[q]$ .
- $\iota \in \text{End}(E)$  such that  $\iota(P) = Q$ .
- $I_P$  is such that  $I_P = I_\varphi$  with  $\ker(\varphi) = \langle P \rangle$ .

1. We can compute  $I_\phi$  for  $\deg(\phi) = q$ .

$$\ker(\phi) = \langle [a]P + [b]Q \rangle \implies I_\phi = [a + b\iota]_* I_P$$

2. This is preserved through isogenies.

$$\ker(\phi) = \langle [a]\psi(P) + [b]\psi(Q) \rangle \implies I_\phi = [(a + b\iota)I_\psi]_* I_P$$

# DeuringVRF Basis

- Finding  $I_\phi$  is easy if  $\deg(\phi)$  smooth, but what if  $\deg(\phi)$  non-smooth ?

## DeuringVRF Basis

A **DeuringVRF basis**  $(P, Q, \iota, I_P)$  is:

- $P, Q \in E$  such that  $\langle P, Q \rangle = E[q]$ .
- $\iota \in \text{End}(E)$  such that  $\iota(P) = Q$ .
- $I_P$  is such that  $I_P = I_\varphi$  with  $\ker(\varphi) = \langle P \rangle$ .

1. We can compute  $I_\phi$  for  $\deg(\phi) = q$ .

$$\ker(\phi) = \langle [a]P + [b]Q \rangle \implies I_\phi = [a + b\iota]_* I_P$$

2. This is preserved through isogenies.

$$\ker(\phi) = \langle [a]\psi(P) + [b]\psi(Q) \rangle \implies I_\phi = [(a + b\iota)I_\psi]_* I_P$$

# DeuringVRF Basis

- Finding  $I_\phi$  is easy if  $\deg(\phi)$  smooth, but what if  $\deg(\phi)$  non-smooth ?

## DeuringVRF Basis

A **DeuringVRF basis**  $(P, Q, \iota, I_P)$  is:

- $P, Q \in E$  such that  $\langle P, Q \rangle = E[q]$ .
- $\iota \in \text{End}(E)$  such that  $\iota(P) = Q$ .
- $I_P$  is such that  $I_P = I_\varphi$  with  $\ker(\varphi) = \langle P \rangle$ .

1. We can compute  $I_\phi$  for  $\deg(\phi) = q$ .

$$\ker(\phi) = \langle [a]P + [b]Q \rangle \implies I_\phi = [a + b\iota]_* I_P$$

2. This is preserved through isogenies.

$$\ker(\phi) = \langle [a]\psi(P) + [b]\psi(Q) \rangle \implies I_\phi = [(a + b\iota)I_\psi]_* I_P$$



# DeuringVRF Basis

- Finding  $I_\phi$  is easy if  $\deg(\phi)$  smooth, but what if  $\deg(\phi)$  non-smooth ?

## DeuringVRF Basis

A **DeuringVRF basis**  $(P, Q, \iota, I_P)$  is:

- $P, Q \in E$  such that  $\langle P, Q \rangle = E[q]$ .
- $\iota \in \text{End}(E)$  such that  $\iota(P) = Q$ .
- $I_P$  is such that  $I_P = I_\varphi$  with  $\ker(\varphi) = \langle P \rangle$ .

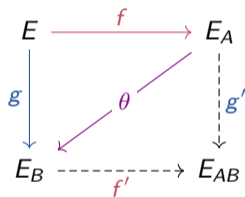
1. We can compute  $I_\phi$  for  $\deg(\phi) = q$ .

$$\ker(\phi) = \langle [a]P + [b]Q \rangle \implies I_\phi = [a + b\iota]_* I_P$$

2. This is preserved through isogenies.

$$\ker(\phi) = \langle [a]\psi(P) + [b]\psi(Q) \rangle \implies I_\phi = [(a + b\iota)I_\psi]_* I_P$$

## Kani's Lemma



$$\deg(f) + \deg(g) = a + b = N$$

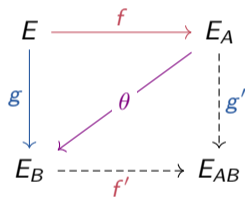
$$\gcd(a, b) = 1$$

 $\implies$ 

$$E_A \times E_B \xrightarrow{F := \begin{pmatrix} \hat{f} & -\hat{g} \\ g' & f' \end{pmatrix}} E \times E_{AB}$$

$$\begin{aligned} \ker(F) &= \left\{ (f(P), -g(P)) \mid P \in E[N] \right\} \\ &= \left\{ ([N-b]P, -\theta(P)) \mid P \in E_A[N] \right\} \end{aligned}$$

## Kani's Lemma



$$\deg(f) + \deg(g) = a + b = N$$

$$\gcd(a, b) = 1$$

 $\implies$ 

$$E_A \times E_B \xrightarrow{F := \begin{pmatrix} \hat{f} & -\hat{g} \\ g' & f' \end{pmatrix}} E \times E_{AB}$$

$$\begin{aligned} \ker(F) &= \left\{ (f(P), -g(P)) \mid P \in E[N] \right\} \\ &= \left\{ ([N-b]P, -\theta(P)) \mid P \in E_A[N] \right\} \end{aligned}$$

# SQIPrime: KeyGen & Commitment

**Public parameters** :  $p + 1 = 2^e f$  with  $q|p - 1$  and  $q \simeq 2^\lambda$  prime.  
 +  $(P, Q, \iota, l_P)$  a *DeuringVRF* basis of  $E_0[q]$

## • Key Generation:

- Sample  $\phi_{sk}, l_{sk}$  of degree  $l_{sk} < 2^e$  prime.
- $\begin{pmatrix} R \\ S \end{pmatrix} = \mathbf{M} \cdot \phi_{sk} \begin{pmatrix} P \\ Q \end{pmatrix}$ .
- $pk = E_{pk}, R, S$      $sk = \phi_{sk}, l_{sk}, \mathbf{M}$ .

 $E_0$ 

## • Commitment:

- Sample  $\phi_{com}, l_{com}$  of degree  $l_{com} < 2^e$  prime.
- Commit  $E_{com}$ .

---


$$\mathbf{M} \in \text{GL}_2(\mathbb{F}_q)$$

# SQIPrime: KeyGen & Commitment

**Public parameters** :  $p + 1 = 2^e f$  with  $q|p - 1$  and  $q \simeq 2^\lambda$  prime.  
 +  $(P, Q, \iota, I_P)$  a *DeuringVRF basis* of  $E_0[q]$

## • Key Generation:

- Sample  $\phi_{sk}, I_{sk}$  of degree  $l_{sk} < 2^e$  prime.
- $\begin{pmatrix} R \\ S \end{pmatrix} = \mathbf{M} \cdot \phi_{sk} \begin{pmatrix} P \\ Q \end{pmatrix}$ .
- $pk = E_{pk}, R, S$      $sk = \phi_{sk}, I_{sk}, \mathbf{M}$ .

## • Commitment:

- Sample  $\phi_{com}, I_{com}$  of degree  $l_{com} < 2^e$  prime.
- Commit  $E_{com}$ .



---


$$\mathbf{M} \in \text{GL}_2(\mathbb{F}_q)$$

# SQIPrime: KeyGen & Commitment

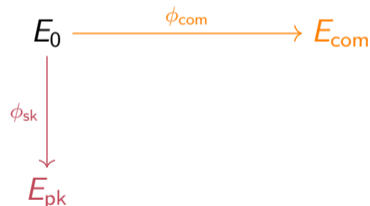
**Public parameters** :  $p + 1 = 2^e f$  with  $q|p - 1$  and  $q \simeq 2^\lambda$  prime.  
 +  $(P, Q, \iota, I_P)$  a *DeuringVRF basis* of  $E_0[q]$

## • Key Generation:

- Sample  $\phi_{sk}, I_{sk}$  of degree  $l_{sk} < 2^e$  prime.
- $\begin{pmatrix} R \\ S \end{pmatrix} = \mathbf{M} \cdot \phi_{sk} \begin{pmatrix} P \\ Q \end{pmatrix}$ .
- $pk = E_{pk}, R, S$      $sk = \phi_{sk}, I_{sk}, \mathbf{M}$ .

## • Commitment:

- Sample  $\phi_{com}, I_{com}$  of degree  $l_{com} < 2^e$  prime.
- Commit  $E_{com}$ .



---


$$\mathbf{M} \in \text{GL}_2(\mathbb{F}_q)$$

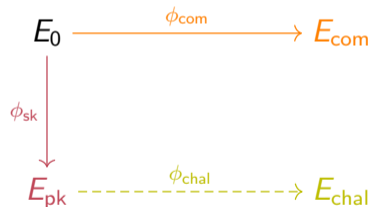
# SQIPrime: Challenge & Response

## • Challenge:

- Challenge is  $a \in \mathbb{Z}_q$ .
- $\ker(\phi_{\text{chal}}) = \langle C_a \rangle = \langle R + [a]S \rangle$ .

## • Response:

- Retrieve  $l_{\text{com}} = [(b + ca)l_{\text{sk}}] * l_p$ .
- Compute  $l_{\text{res}} \sim l_{\text{com}} l_{\text{sk}} l_{\text{com}}$  of norm  $d \leq \sqrt{p}$ .
- Using  $\text{End}(E_0)$  evaluate  $\phi_{\text{chal+res}}(E_{\text{pk}}[2^e])$ .
- Send  $\phi_{\text{chal+res}}(E_{\text{pk}}[2^e])$  (and  $d$ ).



$$R + [a]S = [b]\phi_{\text{sk}}(P) + [c]\phi_{\text{sk}}(Q) \iff \begin{pmatrix} b \\ c \end{pmatrix} = \mathbf{M}^T \begin{pmatrix} 1 \\ a \end{pmatrix}$$

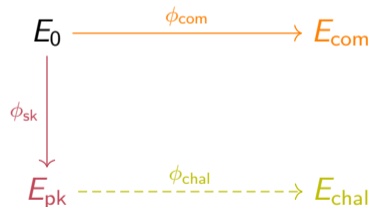
# SQIPrime: Challenge & Response

## • Challenge:

- Challenge is  $a \in \mathbb{Z}_q$ .
- $\ker(\phi_{\text{chal}}) = \langle C_a \rangle = \langle R + [a]S \rangle$ .

## • Response:

- Retrieve  $l_{\text{chal}} = [(b + cl)l_{\text{sk}}]_* l_p$ .
- Compute  $l_{\text{res}} \sim l_{\text{chal}} l_{\text{sk}} l_{\text{com}}$  of norm  $d \leq \sqrt{p}$ .
- Using  $\text{End}(E_0)$  evaluate  $\phi_{\text{chal+res}}(E_{\text{pk}}[2^e])$ .
- Send  $\phi_{\text{chal+res}}(E_{\text{pk}}[2^e])$  (and  $d$ ).



$$R + [a]S = [b]\phi_{\text{sk}}(P) + [c]\phi_{\text{sk}}(Q) \iff \begin{pmatrix} b \\ c \end{pmatrix} = \mathbf{M}^T \begin{pmatrix} 1 \\ a \end{pmatrix}$$



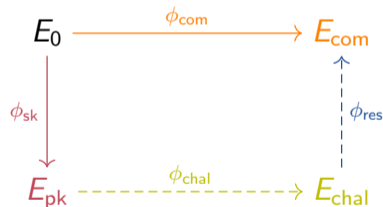
# SQIPrime: Challenge & Response

## • Challenge:

- Challenge is  $a \in \mathbb{Z}_q$ .
- $\ker(\phi_{\text{chal}}) = \langle C_a \rangle = \langle R + [a]S \rangle$ .

## • Response:

- Retrieve  $l_{\text{chal}} = [(b + cl)l_{\text{sk}}]_* l_p$ .
- Compute  $l_{\text{res}} \sim l_{\text{chal}} l_{\text{sk}} l_{\text{com}}$  of norm  $d \leq \sqrt{p}$ .
- Using  $\text{End}(E_0)$  evaluate  $\phi_{\text{chal+res}}(E_{\text{pk}}[2^e])$ .
- Send  $\phi_{\text{chal+res}}(E_{\text{pk}}[2^e])$  (and  $d$ ).



$$R + [a]S = [b]\phi_{\text{sk}}(P) + [c]\phi_{\text{sk}}(Q) \iff \begin{pmatrix} b \\ c \end{pmatrix} = \mathbf{M}^T \begin{pmatrix} 1 \\ a \end{pmatrix}$$

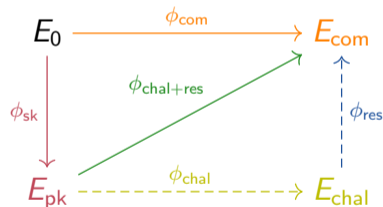
# SQIPrime: Challenge & Response

## • Challenge:

- Challenge is  $a \in \mathbb{Z}_q$ .
- $\ker(\phi_{\text{chal}}) = \langle C_a \rangle = \langle R + [a]S \rangle$ .

## • Response:

- Retrieve  $l_{\text{chal}} = [(b + cl)l_{\text{sk}}]_* l_p$ .
- Compute  $l_{\text{res}} \sim l_{\text{chal}} l_{\text{sk}} l_{\text{com}}$  of norm  $d \leq \sqrt{p}$ .
- Using  $\text{End}(E_0)$  evaluate  $\phi_{\text{chal+res}}(E_{\text{pk}}[2^e])$ .
- Send  $\phi_{\text{chal+res}}(E_{\text{pk}}[2^e])$  (and  $d$ ).



$$R + [a]S = [b]\phi_{\text{sk}}(P) + [c]\phi_{\text{sk}}(Q) \iff \begin{pmatrix} b \\ c \end{pmatrix} = \mathbf{M}^T \begin{pmatrix} 1 \\ a \end{pmatrix}$$

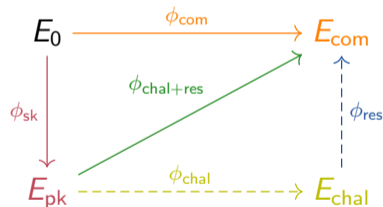
# SQIPrime: Challenge & Response

## Challenge:

- Challenge is  $a \in \mathbb{Z}_q$ .
- $\ker(\phi_{\text{chal}}) = \langle C_a \rangle = \langle R + [a]S \rangle$ .

## Response:

- Retrieve  $l_{\text{chal}} = [(b + cl)l_{\text{sk}}]_* l_p$ .
- Compute  $l_{\text{res}} \sim l_{\text{chal}} l_{\text{sk}} l_{\text{com}}$  of norm  $d \leq \sqrt{p}$ .
- Using  $\text{End}(E_0)$  evaluate  $\phi_{\text{chal+res}}(E_{\text{pk}}[2^e])$ .
- Send  $\phi_{\text{chal+res}}(E_{\text{pk}}[2^e])$  (and  $d$ ).



$$R + [a]S = [b]\phi_{\text{sk}}(P) + [c]\phi_{\text{sk}}(Q) \iff \begin{pmatrix} b \\ c \end{pmatrix} = \mathbf{M}^T \begin{pmatrix} 1 \\ a \end{pmatrix}$$

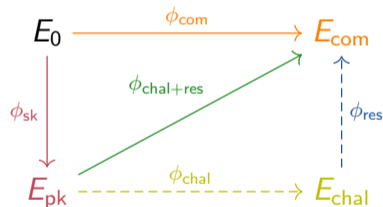
# SQIPrime: Verification idea

- **Verify:**

- Using Kani's Lemma, represent  $\phi_{\text{chal+res}}$ .
- Check  $\phi_{\text{chal+res}}(C_a) \stackrel{?}{=} 0$ .
- ▶ Need an auxiliary isogeny  $\phi_{\text{aux}}$  of degree  $2^e - qd$ .

- **Easy in dim 4:**

- $2^e - qd = a_1^2 + a_2^2 \implies \phi_{\text{aux}} \in \text{End}(E_{\text{pk}}^2)$ .



- **Harder in dim 2:**

- ▶ What if  $\deg(\phi_{\text{sk}}) = q$ ?

---


$$\deg(\phi_{\text{chal+res}}) = qd$$

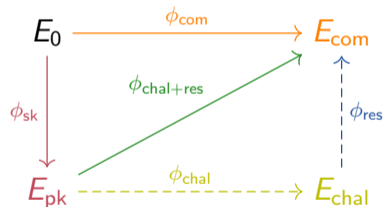
# SQIPrime: Verification idea

- **Verify:**

- Using Kani's Lemma, represent  $\phi_{\text{chal+res}}$ .
- Check  $\phi_{\text{chal+res}}(C_a) \stackrel{?}{=} 0$ .
- ▶ Need an auxiliary isogeny  $\phi_{\text{aux}}$  of degree  $2^e - qd$ .

- **Easy in dim 4:**

- $2^e - qd = a_1^2 + a_2^2 \implies \phi_{\text{aux}} \in \text{End}(E_{\text{pk}}^2)$ .



- **Harder in dim 2:**

- ▶ What if  $\deg(\phi_{\text{sk}}) = q$ ?

---


$$\deg(\phi_{\text{chal+res}}) = qd$$

# SQIPrime: Verification idea

- **Verify:**

- Using Kani's Lemma, represent  $\phi_{\text{chal+res}}$ .
- Check  $\phi_{\text{chal+res}}(C_a) \stackrel{?}{=} 0$ .
- ▶ Need an auxiliary isogeny  $\phi_{\text{aux}}$  of degree  $2^e - qd$ .

- **Easy in dim 4:**

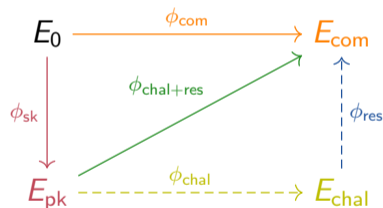
- $2^e - qd = a_1^2 + a_2^2 \implies \phi_{\text{aux}} \in \text{End}(E_{\text{pk}}^2)$ .

$$E_{\text{com}}^2 \times E_{\text{pk}}^2 \xrightarrow{F} E_{\text{pk}}^2 \times E_{\text{com}}^2$$

$$F := \begin{pmatrix} \widehat{\phi_{\text{chal+res}}} & 0 & -a_1 & -a_2 \\ 0 & \widehat{\phi_{\text{chal+res}}} & a_2 & -a_1 \\ a_1 & -a_2 & \phi_{\text{chal+res}} & 0 \\ a_2 & a_1 & 0 & \phi_{\text{chal+res}} \end{pmatrix}$$

- **Harder in dim 2:**

- ▶ What if  $\deg(\phi_{\text{sk}}) = q$ ?



---


$$\deg(\phi_{\text{chal+res}}) = qd$$

# SQIPrime: Verification idea

- **Verify:**

- Using Kani's Lemma, represent  $\phi_{\text{chal+res}}$ .
- Check  $\phi_{\text{chal+res}}(C_a) \stackrel{?}{=} 0$ .
- ▶ Need an auxiliary isogeny  $\phi_{\text{aux}}$  of degree  $2^e - qd$ .

- **Easy in dim 4:**

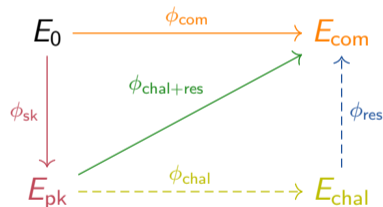
- $2^e - qd = a_1^2 + a_2^2 \implies \phi_{\text{aux}} \in \text{End}(E_{\text{pk}}^2)$ .

$$E_{\text{com}}^2 \times E_{\text{pk}}^2 \xrightarrow{F} E_{\text{pk}}^2 \times E_{\text{com}}^2$$

$$F := \begin{pmatrix} \widehat{\phi_{\text{chal+res}}} & 0 & -a_1 & -a_2 \\ 0 & \widehat{\phi_{\text{chal+res}}} & a_2 & -a_1 \\ a_1 & -a_2 & \phi_{\text{chal+res}} & 0 \\ a_2 & a_1 & 0 & \phi_{\text{chal+res}} \end{pmatrix}$$

- **Harder in dim 2:**

- ▶ What if  $\deg(\phi_{\text{sk}}) = q$ ?



---


$$\deg(\phi_{\text{chal+res}}) = qd$$

# SQIPrime: Verification idea

- **Verify:**

- Using Kani's Lemma, represent  $\phi_{\text{chal+res}}$ .
- Check  $\phi_{\text{chal+res}}(C_a) \stackrel{?}{=} 0$ .
- ▶ Need an auxiliary isogeny  $\phi_{\text{aux}}$  of degree  $2^e - qd$ .

- **Easy in dim 4:**

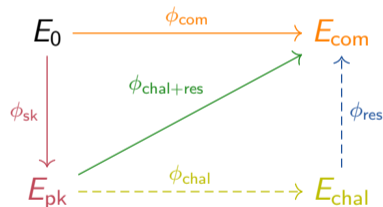
- $2^e - qd = a_1^2 + a_2^2 \implies \phi_{\text{aux}} \in \text{End}(E_{\text{pk}}^2)$ .

$$E_{\text{com}}^2 \times E_{\text{pk}}^2 \xrightarrow{F} E_{\text{pk}}^2 \times E_{\text{com}}^2$$

$$F := \begin{pmatrix} \widehat{\phi_{\text{chal+res}}} & 0 & -a_1 & -a_2 \\ 0 & \widehat{\phi_{\text{chal+res}}} & a_2 & -a_1 \\ a_1 & -a_2 & \phi_{\text{chal+res}} & 0 \\ a_2 & a_1 & 0 & \phi_{\text{chal+res}} \end{pmatrix}$$

- **Harder in dim 2:**

- ▶ What if  $\deg(\phi_{\text{sk}}) = q$ ?



---


$$\deg(\phi_{\text{chal+res}}) = qd$$



# SQIPrime: Verification idea

- **Verify:**

- Using Kani's Lemma, represent  $\phi_{\text{chal+res}}$ .
- Check  $\phi_{\text{chal+res}}(C_a) \stackrel{?}{=} 0$ .
- ▶ Need an auxiliary isogeny  $\phi_{\text{aux}}$  of degree  $2^e - qd$ .

- **Easy in dim 4:**

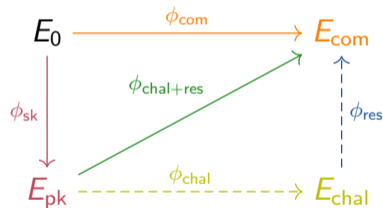
- $2^e - qd = a_1^2 + a_2^2 \implies \phi_{\text{aux}} \in \text{End}(E_{\text{pk}}^2)$ .

$$E_{\text{com}}^2 \times E_{\text{pk}}^2 \xrightarrow{F} E_{\text{pk}}^2 \times E_{\text{com}}^2$$

$$F := \begin{pmatrix} \widehat{\phi_{\text{chal+res}}} & 0 & -a_1 & -a_2 \\ 0 & \widehat{\phi_{\text{chal+res}}} & a_2 & -a_1 \\ a_1 & -a_2 & \phi_{\text{chal+res}} & 0 \\ a_2 & a_1 & 0 & \phi_{\text{chal+res}} \end{pmatrix}$$

- **Harder in dim 2:**

- ▶ What if  $\deg(\phi_{\text{sk}}) = q$ ?

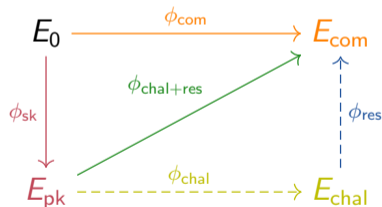


---


$$\deg(\phi_{\text{chal+res}}) = qd$$

# SQIPrime: Auxiliary isogeny

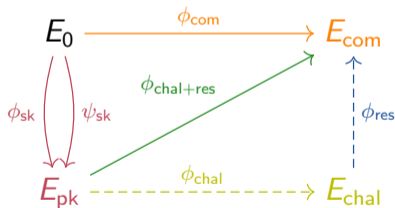
- Need  $\phi_{\text{aux}} : E_{\text{pk}} \rightarrow E_{\text{aux}}$  of degree  $(2^e - qd)$ .
- $\deg(\phi_{\text{sk}}) = q$ .



► More subtle KeyGen and Verification.

# SQIPrime: Auxiliary isogeny

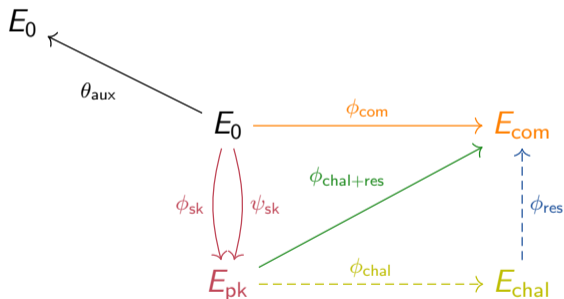
- Need  $\phi_{\text{aux}} : E_{\text{pk}} \rightarrow E_{\text{aux}}$  of degree  $(2^e - qd)$ .
- $\deg(\phi_{\text{sk}}) = q$ .



► More subtle KeyGen and Verification.

# SQIPrime: Auxiliary isogeny

- Need  $\phi_{\text{aux}} : E_{\text{pk}} \rightarrow E_{\text{aux}}$  of degree  $(2^e - qd)$ .
- $\deg(\phi_{\text{sk}}) = q$ .



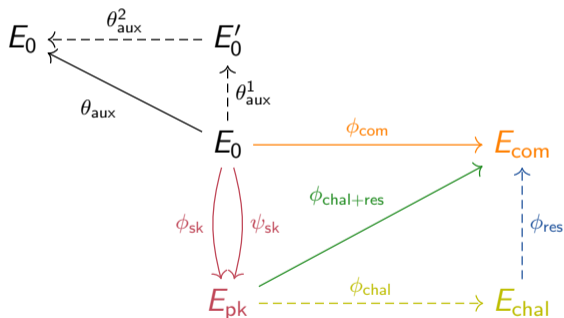
► More subtle KeyGen and Verification.

---


$$\deg(\theta_{\text{com}}) = d(2^e - qd)$$

# SQIPrime: Auxiliary isogeny

- Need  $\phi_{\text{aux}} : E_{\text{pk}} \rightarrow E_{\text{aux}}$  of degree  $(2^e - qd)$ .
- $\deg(\phi_{\text{sk}}) = q$ .

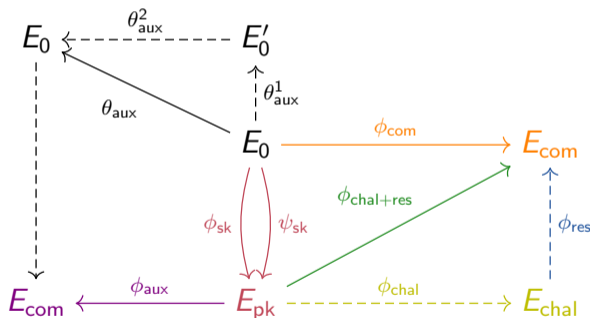


► More subtle KeyGen and Verification.

$$\deg(\theta_{\text{com}}) = d(2^e - qd) \quad , \quad \deg(\theta_{\text{com}}^1) = d \quad , \quad \deg(\theta_{\text{com}}^2) = (2^e - qd)$$

# SQIPrime: Auxiliary isogeny

- Need  $\phi_{\text{aux}} : E_{\text{pk}} \rightarrow E_{\text{com}}$  of degree  $(2^e - qd)$ .
- $\deg(\phi_{\text{sk}}) = q$ .

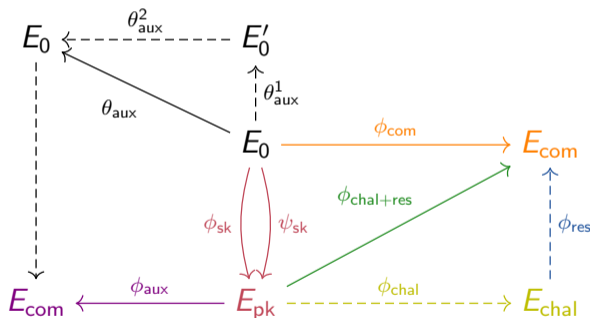


► More subtle KeyGen and Verification.

$$\deg(\theta_{\text{com}}) = d(2^e - qd) \quad , \quad \deg(\theta_{\text{com}}^1) = d \quad , \quad \deg(\theta_{\text{com}}^2) = (2^e - qd)$$

# SQIPrime: Auxiliary isogeny

- Need  $\phi_{\text{aux}} : E_{\text{pk}} \rightarrow E_{\text{com}}$  of degree  $(2^e - qd)$ .
- $\deg(\phi_{\text{sk}}) = q$ .

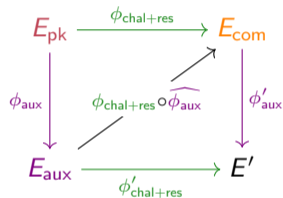


► More subtle KeyGen and Verification.

$$\deg(\theta_{\text{com}}) = d(2^e - qd) \quad , \quad \deg(\theta_{\text{com}}^1) = d \quad , \quad \deg(\theta_{\text{com}}^2) = (2^e - qd)$$

# SQIPrime: Verification

- Given  $\phi_{\text{chal+res}} \circ \widehat{\phi_{\text{aux}}}(E_{\text{aux}}[2^e])$ , we compute  $F$ .
- Verify  $E_{\text{pk}}$  in  $\text{codomain}(F)$ .
- To verify the challenge, we give  $V = \phi_{\text{aux}}(C_a)$ .
- Compute  $\begin{pmatrix} Z_1 \\ Z_2 \end{pmatrix} = F \begin{pmatrix} 0 \\ V \end{pmatrix}$  and check that:
  - $Z_1 = [2^e]C_a$ .
  - $Z_2 = 0$ .

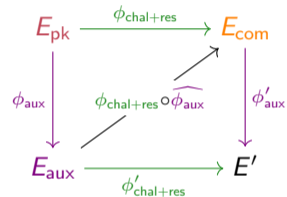


$$E_{\text{com}} \times E_{\text{aux}} \xrightarrow{F := \begin{pmatrix} \widehat{\phi_{\text{chal+res}}} & -\widehat{\phi_{\text{aux}}} \\ \phi'_{\text{aux}} & \phi'_{\text{chal+res}} \end{pmatrix}} E_{\text{pk}} \times E'$$



# SQIPrime: Verification

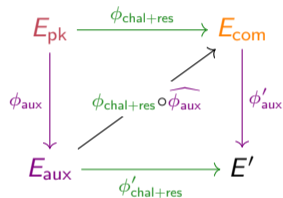
- Given  $\phi_{\text{chal+res}} \circ \widehat{\phi_{\text{aux}}}(E_{\text{aux}}[2^e])$ , we compute  $F$ .
- Verify  $E_{\text{pk}}$  in  $\text{codomain}(F)$ .
- To verify the challenge, we give  $V = \phi_{\text{aux}}(C_a)$ .
- Compute  $\begin{pmatrix} Z_1 \\ Z_2 \end{pmatrix} = F \begin{pmatrix} 0 \\ V \end{pmatrix}$  and check that:
  - $Z_1 = [2^e]C_a$ .
  - $Z_2 = 0$ .



$$E_{\text{com}} \times E_{\text{aux}} \xrightarrow{F := \begin{pmatrix} \phi_{\text{chal+res}} & -\widehat{\phi_{\text{aux}}} \\ \phi'_{\text{aux}} & \phi'_{\text{chal+res}} \end{pmatrix}} E_{\text{pk}} \times E'$$

# SQIPrime: Verification

- Given  $\phi_{\text{chal+res}} \circ \widehat{\phi_{\text{aux}}}(E_{\text{aux}}[2^e])$ , we compute  $F$ .
- Verify  $E_{\text{pk}}$  in  $\text{codomain}(F)$ .
- To verify the challenge, we give  $V = \phi_{\text{aux}}(C_a)$ .
- Compute  $\begin{pmatrix} Z_1 \\ Z_2 \end{pmatrix} = F\begin{pmatrix} 0 \\ V \end{pmatrix}$  and check that:
  - $Z_1 = [2^e]C_a$ .
  - $Z_2 = 0$ .



$$E_{\text{com}} \times E_{\text{aux}} \xrightarrow{F := \begin{pmatrix} \widehat{\phi_{\text{chal+res}}} & -\widehat{\phi_{\text{aux}}} \\ \phi'_{\text{aux}} & \phi'_{\text{chal+res}} \end{pmatrix}} E_{\text{pk}} \times E'$$

# Parameters

- **“SQIPrime”-primes:**  $p$  s.t.  $p + 1 = 2^e f$  with  $q|p - 1$  with  $q \simeq 2^\lambda$  prime.
  - Can be found in polynomial time.

$$p_{117} + 1 = 2^{247} \cdot 79$$

$$p_{130} + 1 = 2^{273} \cdot 19^2$$

$$p_{186} + 1 = 2^{397} \cdot 3^2 \cdot 7^2 \cdot 11^2$$

$$p_{240} + 1 = 2^{499} \cdot 3^2 \cdot 7^2$$

$$q_{117} = 168118140144706967996895604212334429$$

$$q_{130} = (2^{136} \cdot 19 + 1)/955$$

$$q_{186} = (2^{198} \cdot 3 \cdot 7 \cdot 11 - 1)/664723$$

$$q_{240} = (2^{249} \cdot 3 \cdot 7 - 1)/7709$$

# Parameters

- **“SQIPrime”-primes:**  $p$  s.t.  $p + 1 = 2^e f$  with  $q|p - 1$  with  $q \simeq 2^\lambda$  prime.
  - Can be found in polynomial time.

$$p_{117} + 1 = 2^{247} \cdot 79$$

$$p_{130} + 1 = 2^{273} \cdot 19^2$$

$$p_{186} + 1 = 2^{397} \cdot 3^2 \cdot 7^2 \cdot 11^2$$

$$p_{240} + 1 = 2^{499} \cdot 3^2 \cdot 7^2$$

$$q_{117} = 168118140144706967996895604212334429$$

$$q_{130} = (2^{136} \cdot 19 + 1)/955$$

$$q_{186} = (2^{198} \cdot 3 \cdot 7 \cdot 11 - 1)/664723$$

$$q_{240} = (2^{249} \cdot 3 \cdot 7 - 1)/7709$$

# Parameters

- **“SQIPrime”-primes:**  $p$  s.t.  $p + 1 = 2^e f$  with  $q|p - 1$  with  $q \simeq 2^\lambda$  prime.
  - Can be found in polynomial time.

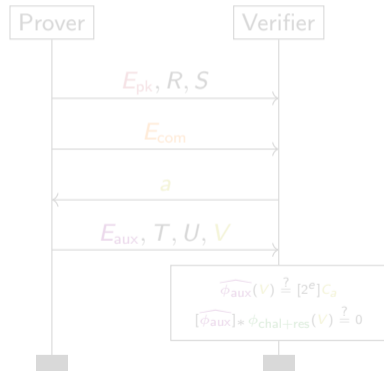
$$\begin{array}{l|l}
 p_{117} + 1 = 2^{247} \cdot 79 & q_{117} = 168118140144706967996895604212334429 \\
 p_{130} + 1 = 2^{273} \cdot 19^2 & q_{130} = (2^{136} \cdot 19 + 1)/955 \\
 p_{186} + 1 = 2^{397} \cdot 3^2 \cdot 7^2 \cdot 11^2 & q_{186} = (2^{198} \cdot 3 \cdot 7 \cdot 11 - 1)/664723 \\
 p_{240} + 1 = 2^{499} \cdot 3^2 \cdot 7^2 & q_{240} = (2^{249} \cdot 3 \cdot 7 - 1)/7709
 \end{array}$$

# SQIPrime as a Signature scheme

- Via Fiat-Shamir, SQIPrime is a quantum resistant signature scheme.

Scheme	$\lambda$	pk	signature	signature (compressed)
SQIPrime	128	191	320	299
	192	288	517	484
	256	384	635	600
SQISign	128	64	322	177
	192	92	-	267
	256	128	-	335
SQISignHD	128	64	208	109
	192	92	312	156
	256	128	416	208
Falcon	128	897	-	666
	256	1793	-	1280

**Table:** Size (in bytes) comparison between the different SQI-protocols.

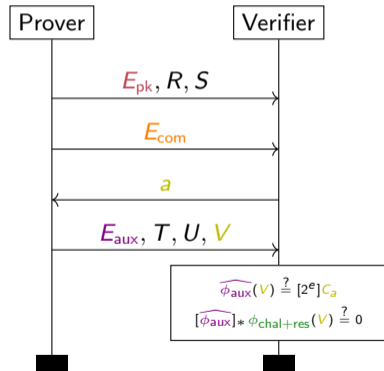


# SQIPrime as a Signature scheme

- Via Fiat-Shamir, SQIPrime is a quantum resistant signature scheme.

Scheme	$\lambda$	pk	signature	signature (compressed)
SQIPrime	128	191	320	299
	192	288	517	484
	256	384	635	600
SQISign	128	64	322	177
	192	92	-	267
	256	128	-	335
SQISignHD	128	64	208	109
	192	92	312	156
	256	128	416	208
Falcon	128	897	-	666
	256	1793	-	1280

**Table:** Size (in bytes) comparison between the different SQI-protocols.



# Efficiency

Scheme	prime	KeyGen	Signature	Verification
ApreSQL	$p_{1973}$	-	335000	-
	$p_7$	-	285000	-
	$p_4$	-	520000	-
SQISignHD	NIST-I	-	-	630
SQIPrime	$p_{117}$	473	677	205
	$p_{130}$	547	804	245
	$p_{186}$	950	1315	382
	$p_{240}$	1427	1927	564

**Table:** Computational times (in ms.) of the different SageMath implementation of SQI-signature schemes, measured on an Apple M1 CPU.



