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.

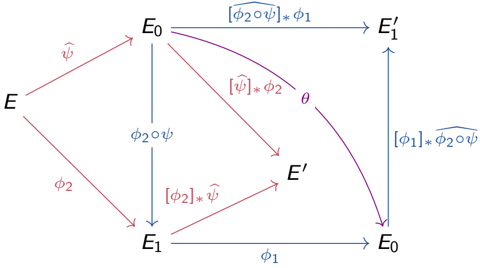
$$
\begin{tikzcd}
 & E_0 \arrow[rr, "{[\widehat{\phi_2\circ\psi}]_*\phi_1}"] \arrow[ddd, "\phi_2\circ\psi"] \arrow[ddr, "{[\widehat{\psi}]_*\phi_2}"] \arrow[dddrr, bend left, "\theta"] & & E_1' \\
E \arrow[ur, "\widehat{\psi}"] \arrow[ddr, "\phi_2"'] & & & \\
 & & E' & \\
 & E_1 \arrow[ur, "{[\phi_2]_*\widehat{\psi}}"] \arrow[rr, "\phi_1"'] & & E_0 \arrow[uuu, "{[\phi_1]_*\widehat{\phi_2\circ\psi}}"']
\end{tikzcd}
$$

SQIPrime

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

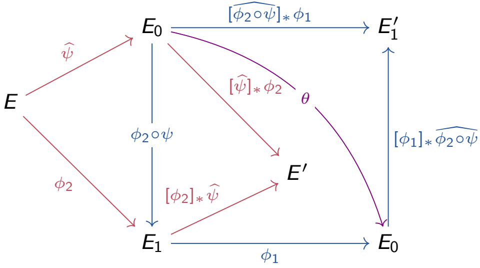
SQIPrime

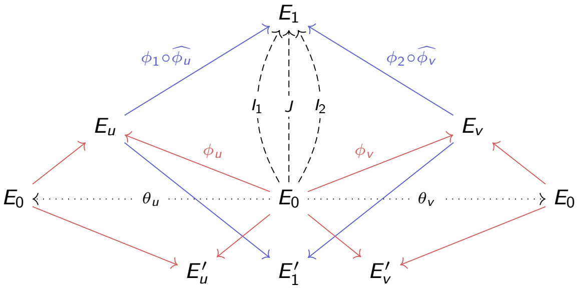
- SQIPrime does SQIsign2D using:
  - Non-smooth challenge isogenies.
  - Kani's Lemma.
  - Diagrams.



SQIPrime

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





DeuringVRF Basis

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

DeuringVRF Basis

A **DeuringVRF basis** (P, Q, ι, I_P) is:

- $P, Q \in E$ such that $\langle P, Q\rangle = E[q]$.
- $\iota \in \mathrm{End}(E)$ 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_ϕ 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_ϕ is easy if $\deg(\phi)$ smooth, but what if $\deg(\phi)$ non-smooth ?

DeuringVRF Basis

A **DeuringVRF basis** (P, Q, ι, I_P) is:

- $P, Q \in E$ such that $\langle P, Q\rangle = E[q]$.
- $\iota \in \mathrm{End}(E)$ 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_ϕ 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_ϕ is easy if $\deg(\phi)$ smooth, but what if $\deg(\phi)$ non-smooth ?

DeuringVRF Basis

A **DeuringVRF basis** (P, Q, ι, I_P) is:

- $P, Q \in E$ such that $\langle P, Q \rangle = E[q]$.
- $\iota \in \mathrm{End}(E)$ 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_ϕ 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_ϕ is easy if $\deg(\phi)$ smooth, but what if $\deg(\phi)$ non-smooth ?

DeuringVRF Basis

A **DeuringVRF basis** (P, Q, ι, I_P) is:

- $P, Q \in E$ such that $\langle P, Q\rangle = E[q]$.
- $\iota \in \mathrm{End}(E)$ 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_ϕ 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

$$
\begin{tikzcd}
E \arrow[r, "f"] \arrow[d, "g"'] & E_A \arrow[dl, "\theta"'] \arrow[d, dashed, "g'"] \\
E_B \arrow[r, dashed, "f'"'] & E_{AB}
\end{tikzcd}
$$

$$\deg(f) + \deg(g) = a + b = N$$
$$\gcd(a, b) = 1$$

$$\Longrightarrow$$

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

$$\ker(F) = \left\{ (f(P), -g(P)) \,\middle|\, P \in E[N] \right\}$$
$$= \left\{ ([N-b]P, -\theta(P)) \,\middle|\, P \in E_A[N] \right\}$$

Kani's Lemma

$$\begin{tikzcd} E \arrow[r, "f"] \arrow[d, "g"'] & E_A \arrow[dl, "\theta"'] \arrow[d, dashed, "g'"] \\ E_B \arrow[r, dashed, "f'"'] & E_{AB} \end{tikzcd}$$

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

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

$$\Longrightarrow$$

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

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

SQIPrime: KeyGen & Commitment

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

- **Key Generation**:
  - Sample $\phi_{\text{sk}}, I_{\text{sk}}$ of degree $\ell_{\text{sk}} < 2^e$ prime.
  - $\binom{R}{S} = \mathbf{M} \cdot \phi_{\text{sk}} \binom{P}{Q}$.
  - $\text{pk} = E_{\text{pk}}, R, S \quad \text{sk} = \phi_{\text{sk}}, I_{\text{sk}}, \mathbf{M}$.

E_0

- **Commitment**:
  - Sample $\phi_{\text{com}}, I_{\text{com}}$ of degree $\ell_{\text{com}} < 2^e$ 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 $\phi_{\mathsf{sk}}, I_{\mathsf{sk}}$ of degree $\ell_{\mathsf{sk}} < 2^e$ prime.
  - $\binom{R}{S} = \mathbf{M} \cdot \phi_{\mathsf{sk}} \binom{P}{Q}$.
  - $\mathsf{pk} = E_{\mathsf{pk}}, R, S \quad \mathsf{sk} = \phi_{\mathsf{sk}}, I_{\mathsf{sk}}, \mathbf{M}$.
- **Commitment**:
  - Sample $\phi_{\mathsf{com}}, I_{\mathsf{com}}$ of degree $\ell_{\mathsf{com}} < 2^e$ prime.
  - Commit E_{com}.

$$\begin{tikzcd} E_0 \arrow[d, "\phi_{\mathsf{sk}}"'] \\ E_{\mathsf{pk}} \end{tikzcd}$$

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

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 $\phi_{\mathsf{sk}}, I_{\mathsf{sk}}$ of degree $\ell_{\mathsf{sk}} < 2^e$ prime.
  - $\binom{R}{S} = \mathbf{M} \cdot \phi_{\mathsf{sk}} \binom{P}{Q}$.
  - $\mathsf{pk} = E_{\mathsf{pk}}, R, S$ $\quad \mathsf{sk} = \phi_{\mathsf{sk}}, I_{\mathsf{sk}}, \mathbf{M}$.
- **Commitment**:
  - Sample $\phi_{\mathsf{com}}, I_{\mathsf{com}}$ of degree $\ell_{\mathsf{com}} < 2^e$ prime.
  - Commit E_{com}.

$$
\begin{tikzcd}
E_0 \arrow[r, "\phi_{\mathsf{com}}"] \arrow[d, "\phi_{\mathsf{sk}}"'] & E_{\mathsf{com}} \\
E_{\mathsf{pk}} &
\end{tikzcd}
$$

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

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 $I_{\text{chal}} = [(b + c\iota) I_{\text{sk}}]_* I_P$.
  - Compute $I_{\text{res}} \sim I_{\text{chal}} I_{\text{sk}} I_{\text{com}}$ 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).

$$\begin{tikzcd} E_0 \arrow[r, "\phi_{\text{com}}"] \arrow[d, "\phi_{\text{sk}}"'] & E_{\text{com}} \\ E_{\text{pk}} \arrow[r, dashed, "\phi_{\text{chal}}"] & E_{\text{chal}} \end{tikzcd}$$

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

SQIPrime: Challenge & Response

- **Challenge**:
  - Challenge is $a \in \mathbb{Z}_q$.
  - $\ker(\phi_{\mathrm{chal}}) = \langle C_a \rangle = \langle R + [a]S \rangle$.
- **Response**:
  - Retrieve $I_{\mathrm{chal}} = [(b + c\iota)I_{\mathrm{sk}}]_* I_P$.
  - Compute $I_{\mathrm{res}} \sim \overline{I_{\mathrm{chal}}} I_{\mathrm{sk}} I_{\mathrm{com}}$ of norm $d \leq \sqrt{p}$.
  - Using $\mathrm{End}(E_0)$ evaluate $\phi_{\mathrm{chal+res}}(E_{\mathrm{pk}}[2^e])$.
  - Send $\phi_{\mathrm{chal+res}}(E_{\mathrm{pk}}[2^e])$ (and d).

$$\begin{tikzcd} E_0 \arrow[r, "\phi_{\mathrm{com}}"] \arrow[d, "\phi_{\mathrm{sk}}"'] & E_{\mathrm{com}} \\ E_{\mathrm{pk}} \arrow[r, dashed, "\phi_{\mathrm{chal}}"] & E_{\mathrm{chal}} \end{tikzcd}$$

$$R + [a]S = [b]\phi_{\mathrm{sk}}(P) + [c]\phi_{\mathrm{sk}}(Q) \iff \binom{b}{c} = \mathbf{M}^\top \binom{1}{a}$$

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 $I_{\text{chal}} = [(b + c\iota) I_{\text{sk}}]_* I_P$.
  - Compute $I_{\text{res}} \sim I_{\text{chal}} I_{\text{sk}} I_{\text{com}}$ 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).

$$
\begin{tikzcd}
E_0 \arrow[r, "\phi_{\text{com}}"] \arrow[d, "\phi_{\text{sk}}"'] & E_{\text{com}} \\
E_{\text{pk}} \arrow[r, dashed, "\phi_{\text{chal}}"] & E_{\text{chal}} \arrow[u, dashed, "\phi_{\text{res}}"']
\end{tikzcd}
$$

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

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 $\underline{I_{\text{chal}}} = [(\underline{b + c\iota}) I_{\text{sk}}]_* I_P$.
  - Compute $I_{\text{res}} \sim I_{\text{chal}} \overline{I_{\text{sk}}} I_{\text{com}}$ 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).

$$\begin{tikzcd}
E_0 \arrow[r, "\phi_{\text{com}}"] \arrow[d, "\phi_{\text{sk}}"'] & E_{\text{com}} \\
E_{\text{pk}} \arrow[ur, "\phi_{\text{chal+res}}"] \arrow[r, dashed, "\phi_{\text{chal}}"] & E_{\text{chal}} \arrow[u, dashed, "\phi_{\text{res}}"']
\end{tikzcd}$$

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

SQIPrime: Challenge & Response

- **Challenge**:
  - Challenge is $a \in \mathbb{Z}_q$.
  - $\ker(\phi_{\mathsf{chal}}) = \langle C_a \rangle = \langle R + [a]S \rangle$.
- **Response**:
  - Retrieve $I_{\mathsf{chal}} = [(b + c\iota)I_{\mathsf{sk}}]_* I_P$.
  - Compute $I_{\mathsf{res}} \sim \overline{I_{\mathsf{chal}}}\,\overline{I_{\mathsf{sk}}} I_{\mathsf{com}}$ of norm $d \leq \sqrt{p}$.
  - Using $\mathrm{End}(E_0)$ evaluate $\phi_{\mathsf{chal+res}}(E_{\mathsf{pk}}[2^e])$.
  - Send $\phi_{\mathsf{chal+res}}(E_{\mathsf{pk}}[2^e])$ (and d).

$$\begin{tikzcd}
E_0 \arrow[rr, "\phi_{\mathsf{com}}"] \arrow[d, "\phi_{\mathsf{sk}}"'] & & E_{\mathsf{com}} \\
E_{\mathsf{pk}} \arrow[rru, "\phi_{\mathsf{chal+res}}"] \arrow[rr, dashed, "\phi_{\mathsf{chal}}"] & & E_{\mathsf{chal}} \arrow[u, dashed, "\phi_{\mathsf{res}}"']
\end{tikzcd}$$

$R + [a]S = [b]\phi_{\mathsf{sk}}(P) + [c]\phi_{\mathsf{sk}}(Q) \iff \binom{b}{c} = \mathbf{M}^\top \binom{1}{a}$

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 ϕ_{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 $\deg(\phi_{\text{sk}}) = q$?

$$\begin{tikzcd} E_0 \arrow[r, "\phi_{\text{com}}"] \arrow[d, "\phi_{\text{sk}}"'] & E_{\text{com}} \\ E_{\text{pk}} \arrow[ur, "\phi_{\text{chal+res}}"] \arrow[r, dashed, "\phi_{\text{chal}}"] & E_{\text{chal}} \arrow[u, dashed, "\phi_{\text{res}}"'] \end{tikzcd}$$

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

SQIPrime: Verification idea

- **Verify**:
  - Using Kani's Lemma, represent $\phi_{\mathrm{chal+res}}$.
  - Check $\phi_{\mathrm{chal+res}}(C_a) \stackrel{?}{=} 0$.
  - ▶ Need an auxiliary isogeny ϕ_{aux} of degree $2^e - qd$.
- **Easy in dim 4**:
  - $2^e - qd = a_1^2 + a_2^2 \implies \phi_{\mathrm{aux}} \in \mathrm{End}(E_{\mathrm{pk}}^2)$.
- **Harder in dim 2**:
  - ▶ What if $\deg(\phi_{\mathrm{sk}}) = q$?

$$
\begin{tikzcd}
E_0 \arrow[r, "\phi_{\mathrm{com}}"] \arrow[d, "\phi_{\mathrm{sk}}"'] & E_{\mathrm{com}} \\
E_{\mathrm{pk}} \arrow[ur, "\phi_{\mathrm{chal+res}}"] \arrow[r, dashed, "\phi_{\mathrm{chal}}"] & E_{\mathrm{chal}} \arrow[u, dashed, "\phi_{\mathrm{res}}"']
\end{tikzcd}
$$

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

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 ϕ_{aux} of degree $2^e - qd$.
- **Easy in dim 4**:
  - $2^e - qd = a_1^2 + a_2^2 \implies \phi_{\text{aux}} \in \text{End}(E_{\text{pk}}^2)$.

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

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

- **Harder in dim 2**:
  - ▶ What if $\deg(\phi_{\text{sk}}) = q$?

$$\begin{tikzcd} E_0 \arrow[r, "\phi_{\text{com}}"] \arrow[d, "\phi_{\text{sk}}"'] & E_{\text{com}} \\ E_{\text{pk}} \arrow[ur, "\phi_{\text{chal+res}}"] \arrow[r, dashed, "\phi_{\text{chal}}"] & E_{\text{chal}} \arrow[u, dashed, "\phi_{\text{res}}"'] \end{tikzcd}$$

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

SQIPrime: Verification idea

- **Verify**:
  - Using Kani's Lemma, represent $\phi_{\mathrm{chal+res}}$.
  - Check $\phi_{\mathrm{chal+res}}(C_a) \stackrel{?}{=} 0$.
  - ▶ Need an auxiliary isogeny ϕ_{aux} of degree $2^e - qd$.
- **Easy in dim 4**:
  - $2^e - qd = a_1^2 + a_2^2 \implies \phi_{\mathrm{aux}} \in \mathrm{End}(E_{\mathrm{pk}}^2)$.

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

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

- **Harder in dim 2**:
  - ▶ What if $\deg(\phi_{\mathrm{sk}}) = q$?

$$\begin{tikzcd} E_0 \arrow[rr, "\phi_{\mathrm{com}}"] \arrow[d, "\phi_{\mathrm{sk}}"'] & & E_{\mathrm{com}} \\ E_{\mathrm{pk}} \arrow[urr, "\phi_{\mathrm{chal+res}}"] \arrow[rr, dashed, "\phi_{\mathrm{chal}}"] & & E_{\mathrm{chal}} \arrow[u, dashed, "\phi_{\mathrm{res}}"'] \end{tikzcd}$$

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

SQIPrime: Verification idea

- **Verify**:
  - Using Kani's Lemma, represent $\phi_{\mathrm{chal+res}}$.
  - Check $\phi_{\mathrm{chal+res}}(C_a) \stackrel{?}{=} 0$.
  - ▶ Need an auxiliary isogeny ϕ_{aux} of degree $2^e - qd$.
- **Easy in dim 4**:
  - $2^e - qd = a_1^2 + a_2^2 \implies \phi_{\mathrm{aux}} \in \mathrm{End}(E_{\mathrm{pk}}^2)$.

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

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

- **Harder in dim 2**:
  - ▶ What if $\deg(\phi_{\mathrm{sk}}) = q$?

$$\begin{tikzcd}
E_0 \arrow[rr, "\phi_{\mathrm{com}}"] \arrow[d, "\phi_{\mathrm{sk}}"'] & & E_{\mathrm{com}} \\
E_{\mathrm{pk}} \arrow[urr, "\phi_{\mathrm{chal+res}}"] \arrow[rr, dashed, "\phi_{\mathrm{chal}}"] & & E_{\mathrm{chal}} \arrow[u, dashed, "\phi_{\mathrm{res}}"']
\end{tikzcd}$$

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

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 ϕ_{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 $\deg(\phi_{\text{sk}}) = q$?

$$\begin{tikzcd} E_0 \arrow[rr, "\phi_{\text{com}}"] \arrow[d, "\phi_{\text{sk}}"'] & & E_{\text{com}} \\ E_{\text{pk}} \arrow[urr, "\phi_{\text{chal+res}}"] \arrow[rr, dashed, "\phi_{\text{chal}}"] & & E_{\text{chal}} \arrow[u, dashed, "\phi_{\text{res}}"'] \end{tikzcd}$$

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

SQIPrime: Auxiliary isogeny

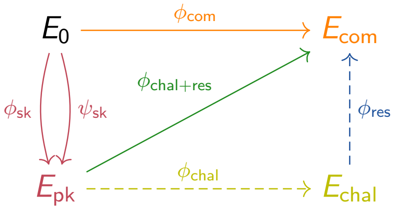
- Need $\phi_{\text{aux}} : E_{\text{pk}} \to E_{\text{aux}}$ of degree $(2^e - qd)$.
- $\deg(\phi_{\text{sk}}) = q$.

$$
\begin{tikzcd}
E_0 \arrow[rr, "\phi_{\text{com}}"] \arrow[d, "\phi_{\text{sk}}"'] & & E_{\text{com}} \\
E_{\text{pk}} \arrow[rru, "\phi_{\text{chal+res}}"] \arrow[rr, dashed, "\phi_{\text{chal}}"] & & E_{\text{chal}} \arrow[u, dashed, "\phi_{\text{res}}"']
\end{tikzcd}
$$

▶ More subtle KeyGen and Verification.

SQIPrime: Auxiliary isogeny

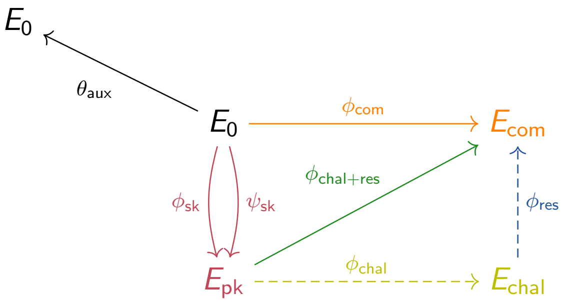
- Need $\phi_{\text{aux}} : E_{\text{pk}} \to E_{\text{aux}}$ of degree $(2^e - qd)$.
- $\deg(\phi_{\text{sk}}) = q$.



- More subtle KeyGen and Verification.

SQIPrime: Auxiliary isogeny

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

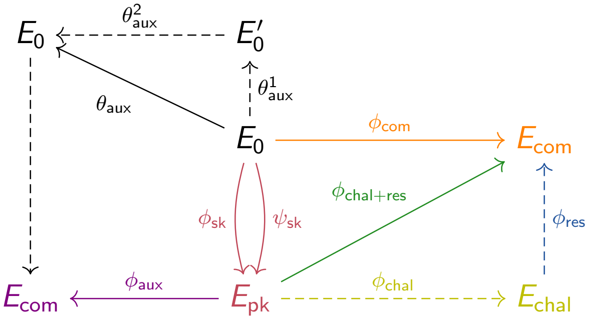
$$
\begin{tikzcd}
E_0 & E_0' \arrow[l, dashed, "\theta^2_{\mathsf{aux}}"'] & \\
 & E_0 \arrow[ul, "\theta_{\mathsf{aux}}"] \arrow[u, dashed, "\theta^1_{\mathsf{aux}}"'] \arrow[r, "\phi_{\mathsf{com}}"] \arrow[d, bend right, "\phi_{\mathsf{sk}}"'] \arrow[d, bend left, "\psi_{\mathsf{sk}}"] & E_{\mathsf{com}} \\
 & E_{\mathsf{pk}} \arrow[ur, "\phi_{\mathsf{chal+res}}"] \arrow[r, dashed, "\phi_{\mathsf{chal}}"] & E_{\mathsf{chal}} \arrow[u, dashed, "\phi_{\mathsf{res}}"']
\end{tikzcd}
$$

▶ More subtle KeyGen and Verification.

$\deg(\theta_{\mathsf{com}}) = d(2^e - qd)$, $\deg(\theta^1_{\mathsf{com}}) = d$, $\deg(\theta^2_{\mathsf{com}}) = (2^e - qd)$

SQIPrime: Auxiliary isogeny

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



▶ More subtle KeyGen and Verification.

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

SQIPrime: Auxiliary isogeny

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

$$
\begin{tikzcd}
E_0 \arrow[dd, dashed] & E_0' \arrow[l, dashed, "\theta^2_{\mathrm{aux}}"'] & \\
 & E_0 \arrow[ul, "\theta_{\mathrm{aux}}"] \arrow[u, dashed, "\theta^1_{\mathrm{aux}}"'] \arrow[r, "\phi_{\mathrm{com}}"] \arrow[d, bend right, "\phi_{\mathrm{sk}}"'] \arrow[d, bend left, "\psi_{\mathrm{sk}}"] & E_{\mathrm{com}} \\
E_{\mathrm{com}} & E_{\mathrm{pk}} \arrow[l, "\phi_{\mathrm{aux}}"'] \arrow[ur, "\phi_{\mathrm{chal+res}}"] \arrow[r, dashed, "\phi_{\mathrm{chal}}"] & E_{\mathrm{chal}} \arrow[u, dashed, "\phi_{\mathrm{res}}"']
\end{tikzcd}
$$

- More subtle KeyGen and Verification.

$\deg(\theta_{\mathrm{com}}) = d(2^e - qd)$, $\deg(\theta^1_{\mathrm{com}}) = d$, $\deg(\theta^2_{\mathrm{com}}) = (2^e - qd)$

SQIPrime: Verification

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

$$
\begin{tikzcd}
E_{\text{pk}} \arrow[r, "\phi_{\text{chal+res}}"] \arrow[d, "\phi_{\text{aux}}"'] & E_{\text{com}} \arrow[d, "\phi'_{\text{aux}}"] \\
E_{\text{aux}} \arrow[r, "\phi'_{\text{chal+res}}"'] \arrow[ur, "\phi_{\text{chal+res}} \circ \widehat{\phi_{\text{aux}}}"] & E'
\end{tikzcd}
$$

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

SQIPrime: Verification

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

$$\begin{tikzcd}
E_{\text{pk}} \arrow[r, "\phi_{\text{chal+res}}"] \arrow[d, "\phi_{\text{aux}}"'] & E_{\text{com}} \arrow[d, "\phi'_{\text{aux}}"] \\
E_{\text{aux}} \arrow[r, "\phi'_{\text{chal+res}}"'] \arrow[ur, "\phi_{\text{chal+res}} \circ \widehat{\phi_{\text{aux}}}"] & E'
\end{tikzcd}$$

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

SQIPrime: Verification

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

$$\begin{tikzcd}
E_{\text{pk}} \arrow[r, "\phi_{\text{chal+res}}"] \arrow[d, "\phi_{\text{aux}}"'] & E_{\text{com}} \arrow[d, "\phi'_{\text{aux}}"] \\
E_{\text{aux}} \arrow[r, "\phi'_{\text{chal+res}}"'] \arrow[ur, "\phi_{\text{chal+res}}\circ\widehat{\phi_{\text{aux}}}"] & E'
\end{tikzcd}$$

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

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.

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

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.

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

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.

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

SQIPrime as a Signature scheme

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

Scheme	λ	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

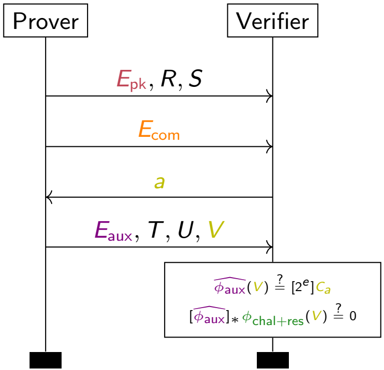
Table: Size (in bytes) comparison between the different SQI-protocols.

SQIPrime as a Signature scheme

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

Scheme	λ	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

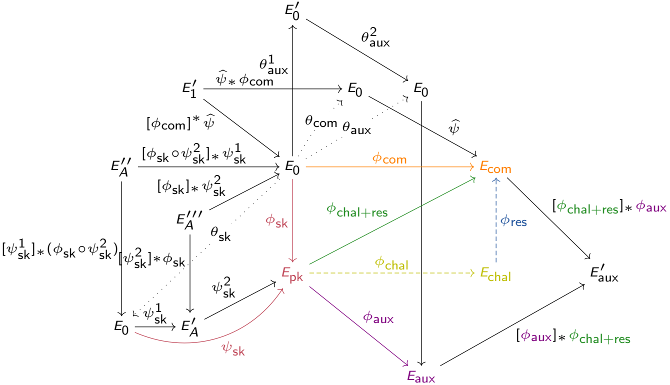
Table: Size (in bytes) comparison between the different SQI-protocols.



Efficiency

Scheme	prime	KeyGen	Signature	Verification
ApreSQI	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.



Paper

This is SQIPrime

Thank you !!

Code