Hash functions from abelian threefolds

Leuven Isogeny Days

Sabrina Kunzweiler, Luciano Maino, Tomoki Moriya, Christophe Petit, Giacomo Pope, Damien Robert, Miha Stopar, Yan Bo Ti

September 13, 2024

The CGL hash function

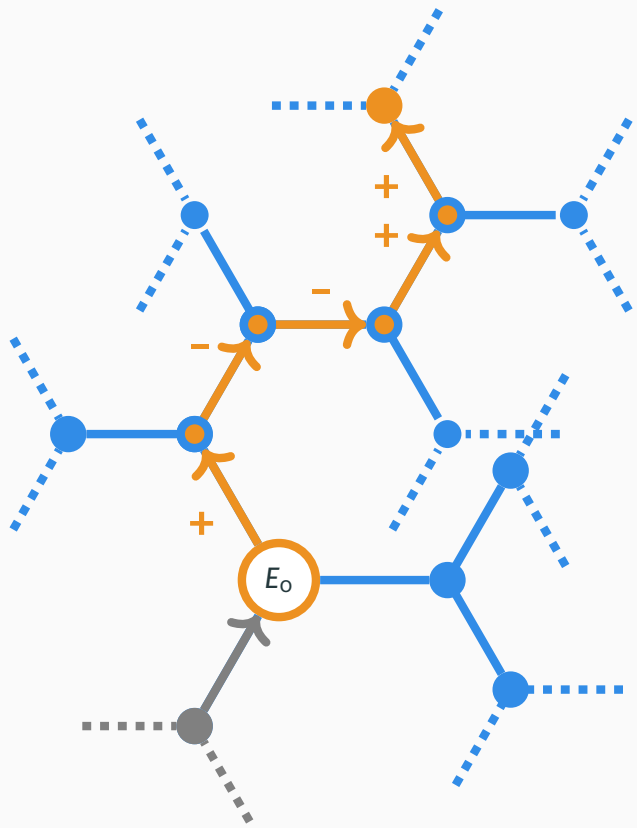
The Charles-Goren-Lauter hash function '08

Setup: supersingular elliptic curve $E_0/\mathbb{F}_{p^2}$
Input: message $(m_1 \dots m_n)$
Output: $H(m) \in \mathbb{F}_{p^2}$

for $i = 1, \dots, n$ **do**
    $E_i = \text{radical2iso}(E_{i-1}, m_i)$
return $j(E_n)$

radical2iso computes a radical 2-isogeny

- cost: essentially one sqrt
- m_i decides the sign of the sqrt



$m = (+ - - + +)$

Security assumptions

Preimage resistance

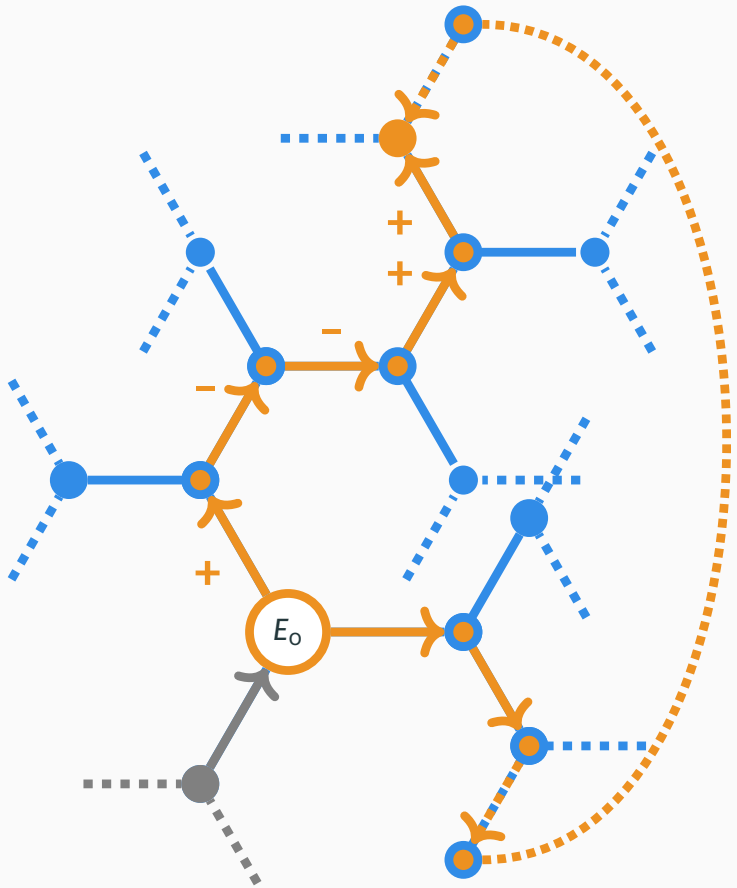
- Given $j \in \mathbb{F}_{p^2}$, it is hard to find m with $H(m) = j$.

$\Rightarrow$ finding a 2^*-isogeny between two supersingular elliptic curves

Collision resistance

- It is hard to find two messages $m \neq m'$ with $H(m) \neq H(m')$.

$\Rightarrow$ finding an endomorphism of degree 2^* of E_0.



CGL in dimension 2

The 2-dimensional setting

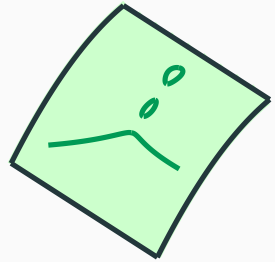
Principally polarized abelian surfaces

Product of elliptic curves,

$E \times E'$

$\approx p^2$

Jacobian of genus-2 curve C,



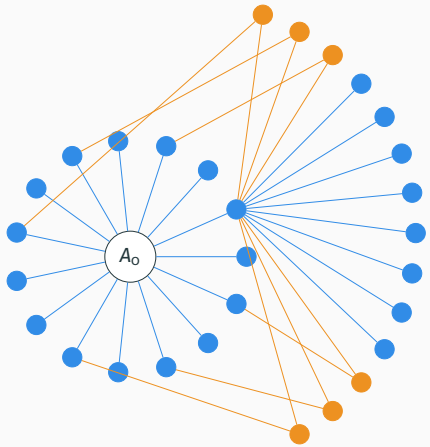
$C : y^2 = f(x)$, $\deg(f) \in \{5, 6\}$.

$\approx p^3$

number of superspecial varieties

(N, N) - Isogenies

- **Kernel**: maximal isotropic subgroup of $A[N]$, isomorphic to $(\mathbb{Z}/N\mathbb{Z})^2$.
- $N = \ell$ prime: $\ell^3 + \ell^2 + \ell + 1$ isotropic (ℓ, ℓ)-groups in total.
- Non-backtracking composition of two (ℓ, ℓ)-isogenies:
  (ℓ^2, ℓ^2)-isogeny , (ℓ^2, ℓ, ℓ)-isogeny



setting for $\ell = 2$

For an (ℓ, ℓ)-isogeny ϕ_1, we are only interested in *good* extensions, i.e. ϕ_2 so that $\phi_2 \circ \phi_1$ is an (ℓ^2, ℓ^2)-isogeny.

$\Rightarrow$ **Multiradical formulas**: explicitly known for $\ell = 2, 3$ (Castryck-Decru '21)

CGL - dim2: Takashima '18, Castryck-Decru-Smith '20

Setup: superspecial abelian surface $A_0/\mathbb{F}_{p^2}$
Input: message $(m_1 \dots m_{3n})$
Output: $H(m) \in \mathbb{F}_{p^2}$

for $i = 1, \dots, n$ **do**
    $A_i = \text{radical2iso}(A_{i-1}, m_{3i-2}, m_{3i-1}, m_{3i})$
return $\text{Igusa}(A_n)$

radical2iso (Richelot)

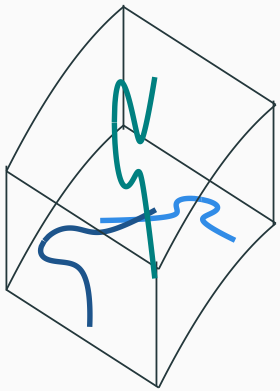
Input: $A = Jac(C)$, $C : y^2 = l_1(x) \cdots l_6(x)$
Output: $A' = Jac(C')$, $C' : y^2 = l'_1(x) \cdots l'_6(x)$.
(1) $g_1 = l_1 \cdot l_4, g_2 = l_2 \cdot l_5, g_3 = l_3 \cdot l_6$
(2) $h_1 = g_2 g'_3 - g_3 g'_2, h_2 = g_3 g'_1 - g_1 g'_3,$
$h_3 = g_1 g'_2 - g_2 g'_1$
(3) $l'_1 \cdot l'_2 = h_1, l'_3 \cdot l'_4 = h_2, l'_5 \cdot l'_6 = h_3$

- cost: essentially 3 sqrts
- $m_{3i-2}, m_{3i-1}, m_{3i}$ decide the signs of the sqrts

The 3-dimensional picture

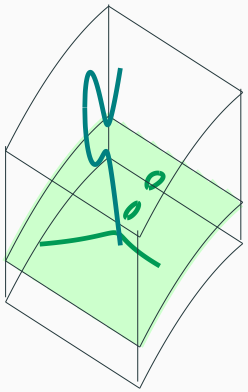
Principally polarized abelian threefolds

reducible threefolds
product of elliptic curve E with abelian surface A



$\approx p^3$

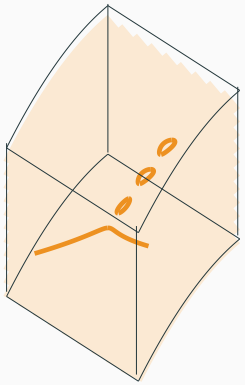
A reducible



$\approx p^4$

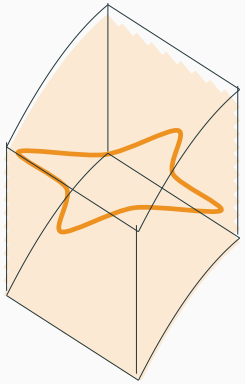
A irreducible

irreducible threefolds
Jacobian of a genus-3 curve C



$\approx p^5$ (?)

C hyperelliptic



$\approx p^6$

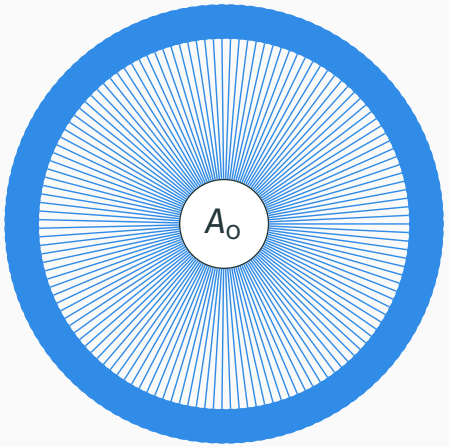
C plane quartic

number of superspecial varieties

Isogenies in dimension 3

(N, N, N)-isogenies

- kernel $G \subset A[N]$ maximal isotropic, and $G \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.
- $N = \ell$ prime: $(\ell^3 + 1)(\ell^2 + 1)(\ell + 1)$ isotropic (ℓ, ℓ, ℓ)-groups of $A[\ell]$ in total.



setting for $\ell = 2$

Computational aspects

- Explicit radical formulas for $\ell = 2$ using theta functions (Ohashi-Onuki-Yoshizumi-Kudo-Nuida '24, this work)

Radical $(2, \ldots, 2)$-isogenies in theta coordinates

$(2,\dots,2)$-isogenies in theta coordinates

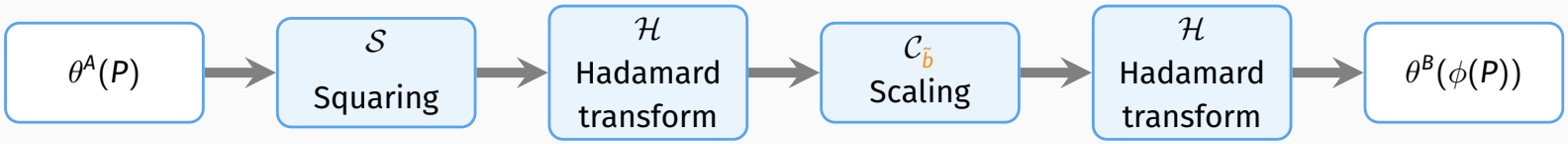
Notation

- A: principally polarized abelian variety of dimension g.
- $\theta^A : A \to \mathbb{P}^{2^g-1}$: a level-2 theta structure.
- $\theta^A(0_A) = (a_0 : \cdots : a_{2^g-1})$: the level-2 theta null point of (A, θ^A).

A maximal 2-isotropic group

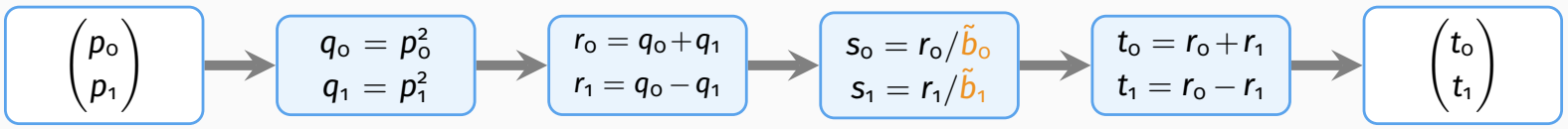
$$G = \langle (a_0 : -a_1 : \cdots : a_{2^g-2} : -a_{2^g-1}), \dots, (a_0 : a_1 : \cdots : -a_{2^g-2} : -a_{2^g-1}) \rangle$$

The $(2,\dots,2)$-isogeny [1] $\phi : A \to B = A/G$



Example: $g = 1$

$\tilde{b}$ dual theta null point of (B, θ^B)



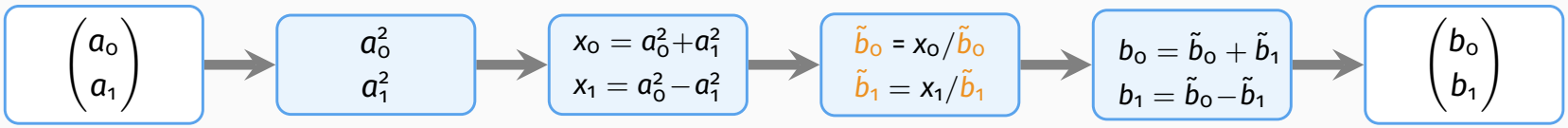
[1] Building block for computing $(2^n, 2^n)$-isogenies (Dartois-Maino-Pope-Robert'24)

Radical formula for $\phi : A \to B$

Goal:
On input $\theta^A(\mathrm{o}_A) = (a_0 : \cdots : a_{2^g-1})$, output $\theta^B(\mathrm{o}_B) = (b_0 : \cdots : b_{2^g-1})$.

Idea: $\mathrm{o}_B = \phi(\mathrm{o}_A)$.

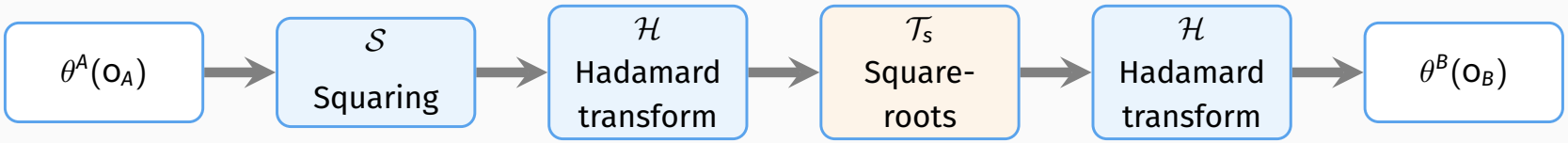
For $g = 1$ $\qquad \tilde{b}_i^2 = x_i$



In general dimension g:

$$\tilde{b}_i^2 = x_i \quad \text{for } i = 0, \ldots, 2^g - 1.$$

Radical isogeny



Compatible square-roots

Essentially: $\mathcal{T}_s : (x_0 : \cdots : x_{2^g-1}) \to (\pm\sqrt{x_0} : \cdots : \pm\sqrt{x_{2^g-1}})$

- Fact: A radical $(2, \ldots, 2)$-isogeny requires $g(g+1)/2$ square-root computations.

⚠ We have $2^g > g(g+1)/2$ coordinates. too many isogenies?

Trick: $(\sqrt{x_0} : \cdots : \sqrt{x_{2^g-1}}) = (x_0 : \sqrt{x_0 x_1} : \cdots : \sqrt{x_0 x_{2^g-1}})$.
$\Rightarrow$ left with $2^g - 1 \geq g(g+1)/2$ square-root computations.

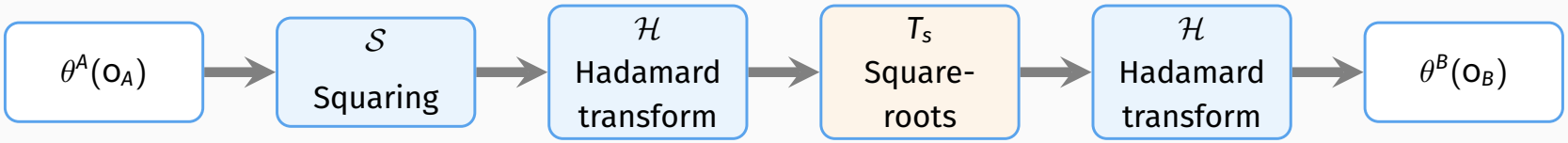
Lemma

Let $I = \{i_1, \ldots, i_{g(g+1)/2}\}$, [a] and assume $x_i \neq 0$ for $i \in I \cap \{0\}$. Then fixing the square-roots $\sqrt{x_0 x_i}$ with $i \in I$, uniquely determines the remaining square-roots.

[a] There are some restrictions on the index set I

Radical isogenies in dimensions 1 and 2

General description



for $g = 1, 2$, we have $2^g - 1 = g(g+1)/2$

dimension 1:

$g(g+1)/2 = 2^g - 1 = 1$

$\mathcal{T}_s : (x_0 : x_1) \mapsto$
$(x_0 : s \cdot \sqrt{x_0 x_1})$

dimension 2:

$g(g+1)/2 = 2^g - 1 = 3$

$\mathcal{T}_s : (x_0 : x_1 : x_2 : x_3) \mapsto$
$(x_0 : s_1 \cdot \sqrt{x_0 x_1} : s_2 \cdot \sqrt{x_0 x_2} : s_3 \cdot \sqrt{x_0 x_3})$

Radical isogenies in dimension 3

$$2^g - 1 = 7 > 6 = g(g+1)/2$$

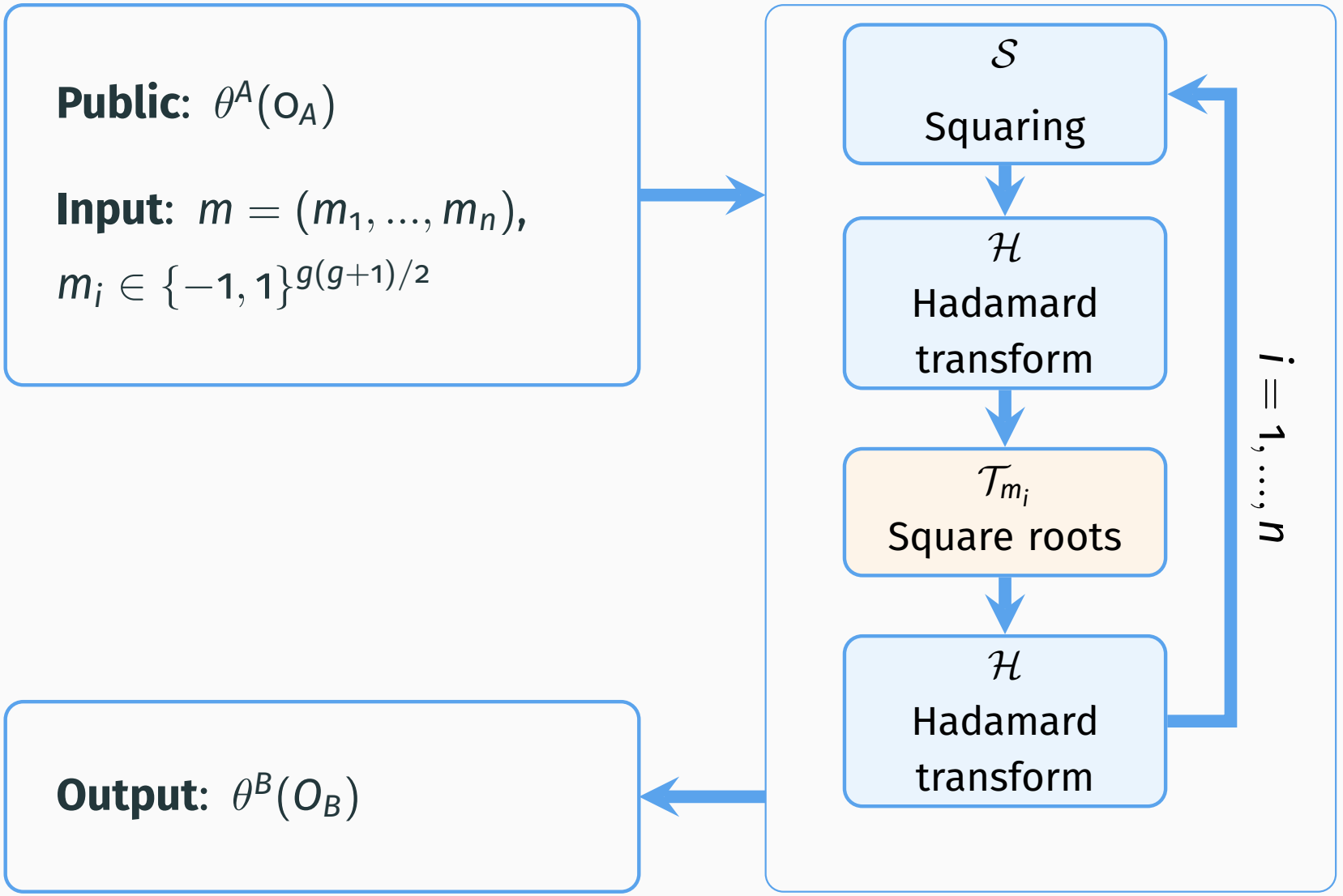
Theorem

$\mathcal{T}_s : (x_0 : \cdots : x_7) \mapsto (x_0 : s_1\sqrt{x_0x_1} : \cdots : s_6\sqrt{x_0x_6} : y_7)$, where
$y_7 = F(s_1\sqrt{x_0x_1}, \ldots, s_6\sqrt{x_0x_6}, x_7)$
for an explicit algebraic expression F.

- **Evaluation of F:** 22 multiplications (in the generic case).
- **Proof idea:** Not all points $(y_0 : \cdots : y_7)$ correspond to a p.p. abelian threefold.
  We use the *Riemann relations* to find a relation $G(y_0, \ldots, y_7) = 0$ among the coordinates of a valid theta null point.

Theta-CGL

Description of our hash function: Theta-CGL$_g$



Why go to dimension $g > 1$?

	$g = 1$	$g = 2$	$g = 3$	$g > 1$
superspecial a.v.s	$\approx p$	$\approx p^3$	$\approx p^6$	$p^{g(g+1)/2}$
solving the isogeny problem	$O(\sqrt{p})$	$O(p)$	$O(p^2)$	$O(p^{g-1})$

Theta-CGL$_g$ with security parameter $\lambda = 128$

A: irreducible superspecial p.p.a.v. over $\mathbb{F}_{p^2}$

	$g = 1$	$g = 2$	$g = 3$	$g > 1$
$\log p$	256	128	64	$\lambda/(g-1)$
computations per bit	$\approx$ 1 sqrt	$\approx$ 1 sqrt	$\approx$ 1 sqrt+	?

Going to higher dimensions allows us to significantly reduce the size of the prime, essentially at no additional cost!

Implementation in Rust

Running times of computing the hash of a 256-bit message in dimensions one, two and three.

	2-radical (μs)	4-radical (μs)	8-radical (μs)
$g = 1$	3153	2037	1737
$g = 2$	989	742	—
$g = 3$	432	—	—

Summary

This presentation

- Explicit formulas for radical $(2, \ldots, 2)$-isogenies in dimensions $g = 1, 2, 3$ using level-2 theta structure.
- Implementation of **Theta-CGL**$_g$ for $g = 1, 2, 3$ showing that dimension 3 is the best setting!

Our (upcoming) paper

- Radical isogeny formulas for 4- and 8-isogenies ($g = 1$)
- Almost radical isogeny formulas for $(4, 4)$-isogenies ($g = 2$)
- Non-generic radical $(2, 2, 2)$-isogeny formulas (e.g. splitting and gluing isogenies).

Thanks for your attention!