# Collisions in isogeny graphs, and the security of the SIDH-based identification protocol


**Federico Pintore**

Department of Mathematics, University of Bari (IT)

Joint work with W. Ghantous (University of Oxford, UK), S. Katsumata (AIST, JP) and M. Veroni (NTNU, NO)


Tor Vergata - Roma - 30/11/2021

# PREVIEW

**SIDH** is the the best-established **isogeny-based cryptosystem**.

An **identification protocol** $\mathrm{ID}_{\mathrm{SIDH}}$ deduced **from SIDH** was turned into **a digital signature scheme** $\mathrm{DS}_{\mathrm{SIDH}}$.

The **security of** $\mathrm{DS}_{\mathrm{SIDH}}$ is **deduced from** two properties of $\mathrm{ID}_{\mathrm{SIDH}}$:
- honest-verifier zero-knowledge
- special soundness.

We dispute the correctness of the proofs for the special soundness in the literature.

# ROADMAP

1. Digital Signatures & Identification Protocols

2. Post-quantum Cryptography, SIDH and $\mathrm{ID}_{\mathrm{SIDH}}$

3. Counterexamples to the special soundness of $\mathrm{ID}_{\mathrm{SIDH}}$

4. Collisions in isogeny graphs

# DIGITAL SIGNATURES

A digital signature is a triple $\mathsf{DS} = (\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$ of PPT algorithms:

- $(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(\lambda)$ : vk is the **verification key**, sk the **secret key**;

- $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, m)$ : it outputs a **signature** on input sk and **a message** $m$;

- $1/0 \leftarrow \mathsf{Verify}(m, \sigma, \mathsf{vk})$ : it deterministically verifies $\sigma$ (on $m$) w.r.t. vk.

# SECURITY OF DIGITAL SIGNATURES

The standard security notion for digital signatures is **existential unforgeability**.

| Challenger $\mathscr{C}$ | | Adversary $\mathscr{A}$ |
|---|---|---|
| $Q := \{\}$ | | |
| $(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(\lambda)$ | $\xrightarrow{\quad \mathsf{vk} \quad}$ | |
| $Q := Q \cup \{m\}$ | $\xleftarrow{\quad m \quad}$ | |
| $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, m)$ | $\xrightarrow{\quad \sigma \quad}$ | |
| | $\dots$ | |
| | $\xleftarrow{\quad (m^*, \sigma^*) \quad}$ | |

$\mathscr{A}$ wins the game if: a) $m^* \notin Q$, b) $1 \leftarrow \mathsf{Verify}(m^*, \sigma^*, \mathsf{vk})$.

$\boxed{\text{DS is existential unforgeable if the winning probability of any } \mathscr{A} \text{ is negligible in } \lambda.}$

# IDENTIFICATION PROTOCOLS

Given $R \subset \mathsf{X} \times \mathsf{W}$, an identification protocol for $R$

$$\mathsf{ID} = (\mathsf{P} = (\mathsf{P}_1, \mathsf{P}_2), \mathsf{V} = (\mathsf{V}_1, \mathsf{V}_2))$$

is a **three-move interactive protocol** between a **prover** (holding a verification-secret key pair $(\mathsf{vk}, \mathsf{sk}) \in R$) and a **verifier** (holding vk).

| **Prover** | | **Verifier** |
|---|---|---|
| $\mathsf{com} \leftarrow \mathsf{P}_1(\mathsf{vk}, \mathsf{sk})$ | $\xrightarrow{\text{com}}$ | |
| | $\xleftarrow{\text{ch}}$ | $\mathsf{ch} \leftarrow \mathsf{V}_1(\mathsf{com})$ |
| $\mathsf{rsp} \leftarrow \mathsf{P}_2(\mathsf{sk}, \mathsf{ch})$ | $\xrightarrow{rsp}$ | |
| | $\xleftarrow{1/0}$ | $1/0 \leftarrow \mathsf{V}_2(\mathsf{com}, \mathsf{ch}, \mathsf{rsp})$ |

# SPECIAL SOUNDNESS OF AN ID

**Required properties:**

- Correctness
- Honest-Verifier Zero-Knowledge
- **Special Soundness**
- …

There exists an **extractor** Ex that, **on input two valid transcripts** $(\mathsf{vk}, \mathsf{com}, \mathsf{ch}, \mathsf{resp}), (\mathsf{vk}, \mathsf{com}, \mathsf{ch}', \mathsf{resp}')$, **outputs** sk s.t. $(\mathsf{vk}, \mathsf{sk}) \in R$.

# FROM AN ID TO A DIGITAL SIGNATURE

When ch varies in an exponential-size set, ID can be turned into a digital signature DS.

- **Fiat-Shamir Transform** → $V_1(\text{com})$ is replaced with $H(m, \text{com})$, where $H$ is a **hash function**.
- Unruh Transform
- Fischlin Transform

If ID satisfies **HVZK** and **special soundness**, and $R$ is a **hard relation** the obtained DS is **existential unforgeable**.

**Proof by reduction**:

- the adversary $\mathscr{A}$ against the unforgeability game is runned twice;
- **thanks to special soundness** sk **is extracted**.

# ROADMAP

1. Identification Protocols & Digital Signatures
2. Post-quantum Cryptography, SIDH and $\mathrm{ID}_{\mathrm{SIDH}}$
3. Counterexamples to the special soundness of $\mathrm{ID}_{\mathrm{SIDH}}$
4. Collisions in isogeny graphs

# POST-QUANTUM CRYPTOGRAPHY

In modern cryptography, security of cryptosystems must be formally proven (**provable security**).

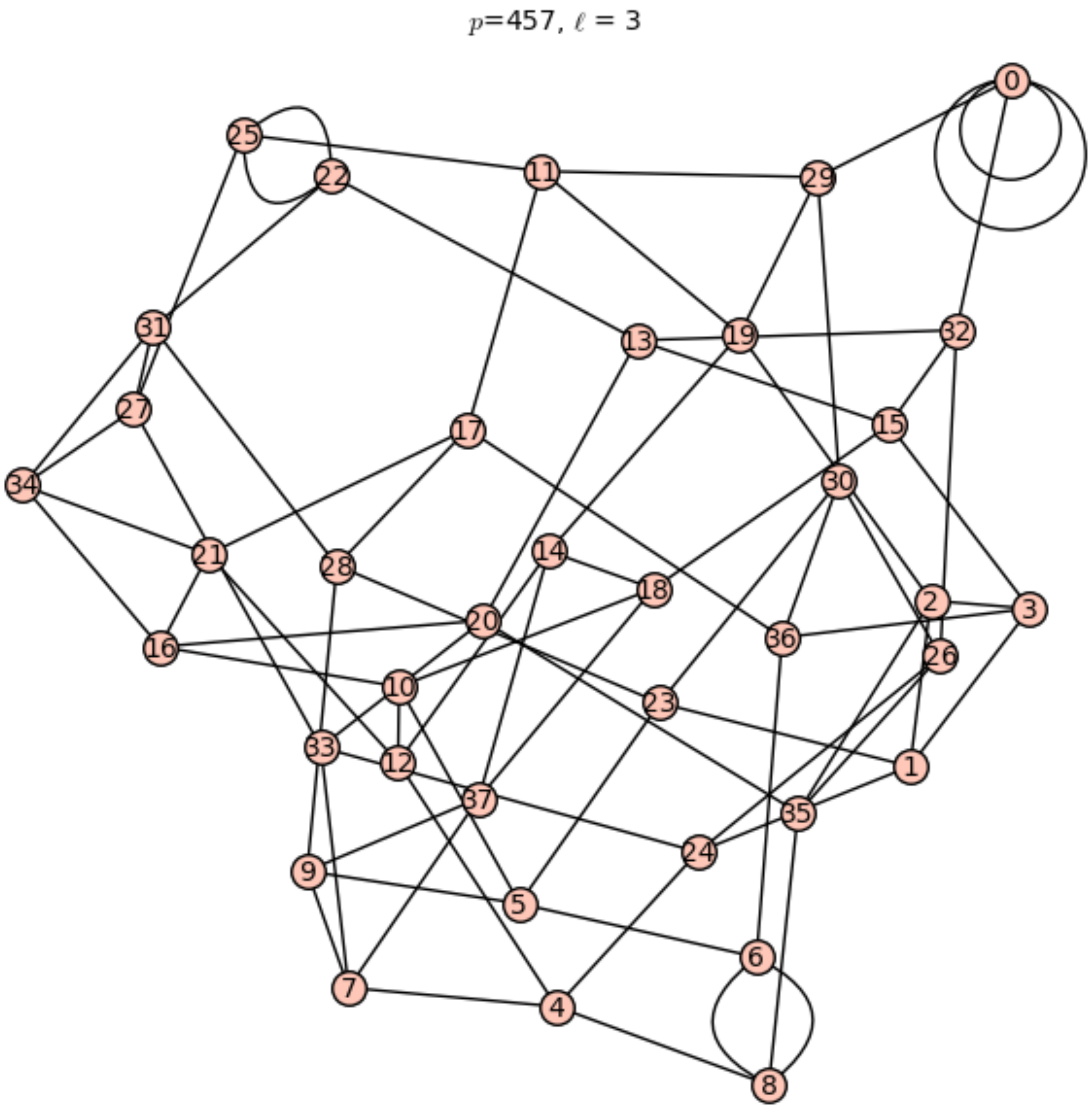
The security proof of a public-key cryptosytem is given under the assumption that a **mathematical problem is hard** (e.g. security of DS obtained from ID).

Hard mathematical problems: integer factorisation, **ECDLP**.

**Shor (1994)**: **quantum algorithms** to solve both problems in **polynomial time**.

**Post-quantum Cryptography**: public-key cryptosystems from **mathematical problems** (supposed to be) **hard** even **for quantum computers**.

# ISOGENY-BASED CRYPTOGRAPHY




Let $p$ be a prime.

**Vertices:** supersingular elliptic curves over $\mathbb{F}_{p^2}$ (modulo isomorphism)

**Edges:** isogenies over $\mathbb{F}_{p^2}$ between elliptic curves (modulo equivalence)

**Isogeny problem:**

given two vertices,

find a path between them.

# ON ELLIPTIC CURVES AND ISOGENIES - 1

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{F}_q$ (i.e. $A, B \in \mathbb{F}_q$). Then

$$E(\overline{\mathbb{F}_q}) = \{(x_0, y_0) \in \overline{\mathbb{F}_q}^2 \mid y_0^2 = x_0^3 + Ax_0 + B\} \cup \{\infty\}$$

is an abelian group.

An isogeny $\varphi : E_0 \to E_1$ is **non-constant morphism** which sends $\infty$ in $\infty$.

$$\downarrow$$

$$\varphi(x, y) \mapsto (f_1(x, y)/f_2(x, y), g_1(x, y)/g_2(x, y))$$

with $f_1, f_2, g_1, g_2 \in \overline{\mathbb{F}_q}[x, y]$

$\deg(\varphi)$ is the degree of $\varphi$ as a morphism. The degree is **multiplicative** w.r.t. $\circ$ (comp.)

# ON ELLIPTIC CURVES AND ISOGENIES - 2

**Isomorphisms** are isogenies of degree 1, which preserve $j$-invariants

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}$$

An **endomorphism** of $E$ is an isogeny $\varphi : E \to E$. (End$(E)$, $+$ , $\circ$ ) is a **ring**.

(End$(E)$, $+$ , $\circ$ ) is **isomorphic** to either an **order** in a quadratic field or a maximal order in a quaternion algebra. In the latter case, $E$ is supersingular.

The number of points of $E$ is predictable

# ON ELLIPTIC CURVES AND ISOGENIES -

An isogeny $\varphi : E_0 \to E_1$ admits a dual $\hat{\varphi} : E_1 \to E_0$ s.t. $\varphi \circ \hat{\varphi} = \hat{\varphi} \circ \varphi = [\deg(\varphi)]$.

Given $G \leqslant E(\overline{\mathbb{F}_q})$, there exists an isogeny $\varphi : E \to E'$ s.t. $\ker(\varphi) = G$.

- $E'$ is denoted by $E/G$
- $E/G$ and $\varphi$ are **unique** modulo isomorphism and equivalence, resp.

If $(\ell, q) = 1$, $E[\ell] = \{P \in E(\overline{\mathbb{F}_q}) \mid [\ell]P = \infty\} \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell$.

# THE SIDH SETTING

- a prime $p = \ell_1^{e_1}\ell_2^{e_2} \pm 1$ ($\ell_1, \ell_2$ small primes)
- a supersingular elliptic curve $E_0$ over $\mathbb{F}_{p^2}$ → $\#E_0(\mathbb{F}_{p^2}) = (\ell_1^{e_1}\ell_2^{e_2})^2$
- $P_1, Q_1$ s.t. $< P_1, Q_1 > = E_0[\ell_1^{e_1}]$
- $P_2, Q_2$ s.t. $< P_2, Q_2 > = E_0[\ell_2^{e_2}]$

**Alice** **Bob**

Samples $m_1 \in \mathbb{Z}_{\ell_1^{e_1}}$

Computes $\varphi_A : E_0 \to E_A = E_0/\langle P_1 + [m_1]Q_1 \rangle$

$$\xrightarrow{E_A, \varphi_A(P_2), \varphi_A(Q_2)}$$

Samples $m_2 \in \mathbb{Z}_{\ell_2^{e_2}}$

Computes $\varphi_B : E_0 \to E_B = E_0/\langle P_2 + [m_2]Q_2 \rangle$

$$\xleftarrow{E_B, \varphi_B(P_1), \varphi_B(Q_1)}$$

$$\boxed{E_B/\langle \varphi_B(P_1) + [m_1]\varphi_B(Q_1) \rangle \simeq E_A/\langle \varphi_A(P_2) + [m_2]\varphi_A(Q_2) \rangle}$$

# THE IDENTIFICATION PROTOCOL ID$_{\text{SIDH}}$

$X = \{(E_1, P', Q') \mid E_1 \text{ sup. } \wedge \langle P', Q' \rangle = E_1[\ell_2^{e_2}]\}$

$Y = \{\varphi \mid \varphi \text{ cyclic isog.}\}$

$R = \{((E_1, P', Q'), \varphi) \mid \varphi : E_0 \to E_1 \wedge \deg(\varphi) = \ell_1^{e_1} \wedge \varphi(P_2) = P', \varphi(Q_2) = Q'\}$

| **Prover** | | **Verifier** |
|---|---|---|
| $(\text{vk} = (E_1, P', Q'), \text{sk} = \varphi)$ | | $\text{vk} = (E_1, P', Q')$ |
| $m_2 \in \mathbb{Z}_{\ell_2^{e_2}}$ | $\xrightarrow{\text{com} = (E_2, E_3)}$ | |
| | $\xleftarrow{\text{ch}}$ | $\text{ch} \leftarrow \{0,1\}$ |
| $\text{rsp} = \begin{cases} m_2 & \text{if ch} = 0 \\ \phi(\ker(\varphi)) & \text{if ch} = 1 \end{cases}$ | $\xrightarrow{\text{rsp}}$ | |
| | $\xleftarrow{1/0}$ | $1/0 \leftarrow \text{V}_2(\text{com}, \text{ch}, \text{rsp})$ |

$$\begin{tikzcd} E_0 \arrow[r, dashed, "\varphi"'] \arrow[d, "\phi"', "\langle P_2 + [m_2]Q_2 \rangle"] & E_1 \arrow[d, "\phi", "\langle P' + [m_2]Q' \rangle"'] \\ E_2 \arrow[r, "\psi"] & E_3 \end{tikzcd}$$

# (CLAIMED) SPECIAL SOUNDNESS OF ID$_{\text{SIDH}}$

$$\begin{tikzcd}
E_0 \arrow[r, dashed, "\varphi"'] \arrow[d, "\langle P_2 + [m_2]Q_2 \rangle"', "\phi"] & E_1 \arrow[d, "\phi'"', "\langle P' + [m_2]Q' \rangle"] \\
E_2 \arrow[r, "\psi", "\langle T \rangle"'] & E_3
\end{tikzcd}$$

$\boxed{\text{Two valid transcripts give the isogeny } \hat{\phi}' \circ \psi \circ \phi \text{ between } E_0 \text{ and } E_1}$

In four papers, the special soundness of ID$_{\text{SIDH}}$ is proven by means of the extractor

$$\hat{\phi}(T) \leftarrow \mathsf{Ex}_{\text{SIDH}}(\phi, \psi, \phi')$$

$$\|$$

$$\ker\left(\hat{\phi}' \circ \psi \circ \phi\right) \cap E_0[\ell_1^{e_1}]$$

# ROADMAP

1. Identification Protocols & Digital Signatures ✓

2. Post-quantum Cryptography, SIDH and $\mathrm{ID}_{\mathrm{SIDH}}$ ✓

3. Counterexamples to the special soundness of $\mathrm{ID}_{\mathrm{SIDH}}$

4. Collisions in isogeny graphs

# COUNTEREXAMPLES TO SPECIAL SOUNDNESS

Let

$$\psi : E_2 = E_0/\langle P_2 + [m_2]Q_2 \rangle \to E_3 = E_1/\langle P' + [m_2]Q' \rangle$$

be the isogeny with kernel $\phi(\ker(\varphi))$

Suppose there exists $\tilde{\psi} : E_2 \to E_3$ cyclic, non equivalent to $\psi$, with $\ker(\tilde{\psi}) = \langle \tilde{T} \rangle$ and $\deg(\tilde{\psi}) = \ell_1^{e_1}$.

$$\begin{tikzcd} E_2 \arrow[rr, "\psi"] \arrow[rr, bend right, "\tilde{\psi}"'] & & E_3 \end{tikzcd}$$

$((E_1, P', Q'), (E_2, E_3), 1, \tilde{T})$ is a **valid transcript!**

| |
|---|
| On input $(\phi, \tilde{\psi}, \phi')$, Ex$_{\text{SIDH}}$ does not output a **valid secret key** for $(E_1, P', Q')$ |

# CONCRETE COUNTEREXAMPLES TO SPECIAL SOUNDNESS - 1

The scenario described in the previous slide is **not** only **theoretical**.

We obtained a **concrete instance** for the biggest set of parameters for SIDH, i.e. $p_{751}$.

The instance considers $E_2 = E_0$, with $j(E_0) = 0$, for which $\mathrm{End}(E_0)$ is known.

> The alternative isogeny $\tilde{\psi}$ is found by looking for a **cyclic endomorphism of degree** $\ell_1^{2e_1}$

This corresponds to the **resolution of a norm equation** in the quaternion algebra.

# COUNTEREXAMPLES TO SPECIAL SOUNDNESS

**Theorem** (Ghantous, Katsumata, _ , Veroni - 2021)

The inputs that make the extractor $\mathrm{Ex}_{\mathrm{SIDH}}$ fail are

precisely those that fall within the framework we described.

# ROADMAP

1. Identification Protocols & Digital Signatures ✓
2. Post-quantum Cryptography, SIDH and $ID_{SIDH}$ ✓
3. Counterexamples to the special soundness of $ID_{SIDH}$ ✓
4. Collisions in isogeny graphs

# MITIGATIONS FOR $DS_{SIDH}$

Replace special soundness with **relaxed special soundness**.

A bigger relation $\tilde{R}$, with $R \subseteq \tilde{R}$, is considered. The extractor Ex is only required to extract sk such that $(\text{vk}, \text{sk}) \in \tilde{R}$.

As long as $\tilde{R}$ is a hard relation, the digital signature from ID is existential unforgeable.

$$\tilde{R} = \{((E_1, P', Q'), \varphi) \,|\, \varphi : E_0 \to E_1\}$$

The problem of computing **any** isogeny between
$E_0$ and $E_1$ is supposed to be hard even for quantum computers

# QUANTIFYING COLLISIONS IN ISOGENY GRAPHS

Given the distinct primes $p$, $\ell$ and $e \in \mathbb{N}$, we call **collision in $\mathscr{G}_{p^2}(\ell)$** any pair of non-equivalent cyclic isogenies $\psi, \tilde{\psi} : E \to E_1$ with $\deg(\psi) = \deg(\tilde{\psi}) = \ell^e$.

We denote by $\mathrm{Coll}_{\ell^e}(E)$ the number of such collisions originating from the curve $E$

Collisions in $\mathscr{G}_{p^2}(\ell)$ are related to endomorphisms of degree $\ell^{2e}$, which are quantified by the **Brandt matrix of degree $\ell^{2e}$.**

We denote by $\mathscr{C}_E(\ell^{2e})$ the number of cyclic endomorphisms of $E$.

# QUANTIFYING COLLISIONS IN ISOGENY GRAPHS

**Lemma** (Ghantous, Katsumata, _ , Veroni - 2021)

$$\mathscr{C}_E(\ell^{2e}) \leq \mathrm{Coll}_{\ell^e}(E) \leq \mathscr{C}_E(\ell^{2e}) + \sum_{r=1}^{e-1} \mathscr{C}_E(\ell^{2r})(\ell - 1)\ell^{e-1-r}$$

Let $n$ be the number of vertices of $\mathscr{G}_{p^2}(\ell)$, which is approximately $p/12$.

**Lemma** (Ghantous, Katsumata, _ , Veroni - 2021)

$$\sum_{i=1}^{n} \mathscr{C}_{E_{(i)}}(\ell^{2e}) \leq \frac{\ell^{2e+1}}{\ell - 1}$$

# QUANTIFYING COLLISIONS IN ISOGENY GRAPHS

**Theorem** (Ghantous, Katsumata, _ , Veroni - 2021)

$$\sum_{i=1}^{n} \mathrm{Coll}_{\ell^e}(E_{(i)}) \leq \frac{\ell^{2e}(\ell+1)}{\ell-1}.$$

**Corollary** (Ghantous, Katsumata, _ , Veroni - 2021)

$$\mathbb{E}_E[\mathrm{Coll}_{\ell^e}(E)] := \frac{1}{n}\sum_{i=1}^{n} \mathrm{Coll}_{\ell^e}(E_{(i)}) \leq \frac{\ell^{2e}(\ell+1)}{n(\ell-1)}.$$

When $p \approx \ell^{2e}$ (SIDH setting), the upper bound of the above expectation is in $\mathcal{O}(1)$.

# QUANTIFYING COLLISIONS IN ISOGENY GRAPHS

Obtaining lower bounds is trickier, as it involves incomplete character sums.

By considering a statistical model which makes use of Bernoulli random variables we obtained the following.

**Theorem** (Ghantous, Katsumata, _ , Veroni - 2021)

$$\frac{1}{4n}\ell^{e-1}(\ell+1)(2\ell^e-1) \leq \mathbb{E}_E(\mathrm{Coll}_{\ell^e}(E))$$

When $p \approx \ell^{2e}$ (SIDH setting), the lower bound of the above expectation is in $\mathcal{O}(1)$.

# Thanks for your attention

**Federico Pintore**
Department of Mathematics, University of Bari (IT)

federico.pintore@uniba.it