Lossy CSI-FISH:

a practical and provable secure isogeny-based signature

Federico Pintore

Mathematical Institute, University of Oxford, UK

Joint work with Ali El Kaafarani[1] and Schuichi Katsumata[2]

[1]Mathematical Institute, University of Oxford (UK) and PQShield (UK)
[2]National Institute of Advanced Industrial Science and Technology (AIST), JP

Turin - 1st July 2020

PRELIMINARIES

Digital signatures are public-key cryptosystems

PRELIMINARIES

Digital signatures are public-key cryptosystems

Security of public-key cryptosystems must be formally proven (**provable security**)

PRELIMINARIES

Digital signatures are public-key cryptosystems

Security of public-key cryptosystems must be formally proven (**provable security**)

Security proofs given under the assumption that a **mathematical problem is hard**

PRELIMINARIES

Digital signatures are public-key cryptosystems

Security of public-key cryptosystems must be formally proven (**provable security**)

Security proofs given under the assumption that a **mathematical problem is hard**

Discrete logarithm problem over elliptic curves (ECDLP) supposed hard

PRELIMINARIES

Elliptic Curve Cryptography (ECC): cryptosystems from the ECDLP assumption

PRELIMINARIES

Elliptic Curve Cryptography (ECC): cryptosystems from the ECDLP assumption

P. Shor (1994): quantum algorithm to solve the ECDLP in polynomial time

PRELIMINARIES

Elliptic Curve Cryptography (ECC): cryptosystems from the ECDLP assumption

P. Shor (1994): quantum algorithm to solve the ECDLP in polynomial time

The concrete possibility to construct quantum computers **threatens ECC**

PRELIMINARIES

Elliptic Curve Cryptography (ECC): cryptosystems from the ECDLP assumption

P. Shor (1994): quantum algorithm to solve the ECDLP in polynomial time

The concrete possibility to construct quantum computers **threatens ECC**

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

PRELIMINARIES

Elliptic Curve Cryptography (ECC): cryptosystems from the ECDLP assumption

P. Shor (1994): quantum algorithm to solve the ECDLP in polynomial time

The concrete possibility to construct quantum computers **threatens ECC**

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

There is the need of new mathematical problems, hard for quantum computers

PRELIMINARIES

Elliptic Curve Cryptography (ECC): cryptosystems from the ECDLP assumption

P. Shor (1994): quantum algorithm to solve the ECDLP in polynomial time

The concrete possibility to construct quantum computers **threatens ECC**

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

There is the need of new mathematical problems, hard for quantum computers

Isogeny problem over elliptic curves supposed hard for quantum computers

PRELIMINARIES

Isogeny-based Cryptography: post-quantum schemes from the isogeny problem

- appealing solutions for **encryption** and **key-exchange**
- rather elusive to construct **digital signatures**

PRELIMINARIES

Isogeny-based Cryptography: post-quantum schemes from the isogeny problem

- appealing solutions for **encryption** and **key-exchange**
- rather elusive to construct **digital signatures**

2011 - First efficient isogeny-based cryptosystem

2019 - First efficient isogeny-based **digital signature: CSI-FiSh**

PRELIMINARIES

Isogeny-based Cryptography: post-quantum schemes from the isogeny problem

- appealing solutions for **encryption** and **key-exchange**
- rather elusive to construct **digital signatures**

2011 - First efficient isogeny-based cryptosystem

2019 - First efficient isogeny-based **digital signature: CSI-FiSh**

Problem: provable security of CSI-FiSh is rather weak (non-tight proof)

TIGHTNESS OF SECURITY PROOFS

An attacker able to break a cryptosystem **CS** with success probability $2^{-\delta_{CS}}$

can solve the hard problem **P** with success probability $2^{-\delta}$, where $2^{-\delta} \leq 2^{-\delta_{CS}}$

TIGHTNESS OF SECURITY PROOFS

An attacker able to break a cryptosystem **CS** with **success probability** $2^{-\delta_{CS}}$

can solve the hard problem **P** with **success probability** $2^{-\delta}$, where $2^{-\delta} \leq 2^{-\delta_{CS}}$

Example - CSI-FiSh

- $2\delta_{\text{CS}} + \log_2 Q_{\text{RO}} = \delta$ <u>(classical attacker)</u>
- Best know algorithm for solving **P** has $\delta = 128$
- $2\delta_{\text{CS}} + \log_2 Q_{\text{RO}} = \delta \geq 128 \Rightarrow \delta_{\text{CS}} \geq (128 - \log_2 Q_{\text{RO}})/2$
- Assuming a rather modest $\log_2 Q_{\text{RO}} = 40$ we have $\delta_{\text{CS}} \geq (128 - 40)/2 = 44$

ISOGENY-BASED CRYPTOGRAPHY AND DIGITAL SIGNATURES: A FRAGILE RELATIONSHIP

Problem: the security proof does not guarantee more than 44 bits of security

ISOGENY-BASED CRYPTOGRAPHY AND DIGITAL SIGNATURES: A FRAGILE RELATIONSHIP

Problem: the security proof does not guarantee more than 44 bits of security

Bigger Problem: CSI-FiSh does not guarantee any bits of provable security

when we consider a quantum attacker $(3\delta_{\mathrm{CS}} + 6\log_2 Q_{\mathrm{QRO}} = \delta)$

ISOGENY-BASED CRYPTOGRAPHY AND DIGITAL SIGNATURES: A FRAGILE RELATIONSHIP

Problem: the security proof does not guarantee more than 44 bits of security

Bigger Problem: CSI-FiSh does not guarantee any bits of provable security when we consider a quantum attacker ($3\delta_{\mathrm{CS}} + 6\log_2 Q_{\mathrm{QRO}} = \delta$)

Increasing the parameters would increase δ (tradeoff with efficiency), but **CSI-FiSh is specific to one set of parameters (CSIDH-512)!**

ISOGENY-BASED CRYPTOGRAPHY AND DIGITAL SIGNATURES: A FRAGILE RELATIONSHIP

Problem: the security proof does not guarantee more than 44 bits of security

Bigger Problem: CSI-FiSh does not guarantee any bits of provable security when we consider a quantum attacker ($3\delta_{\text{CS}} + 6\log_2 Q_{\text{QRO}} = \delta$)

Increasing the parameters would increase δ (tradeoff with efficiency), but **CSI-FiSh is specific to one set of parameters (CSIDH-512)!**

A **better security proof** was needed

OUR CONTRIBUTION: LOSSY CSI-FISH

We propose a **new signature scheme**, Lossy CSI-FiSh, which is

- tightly secure under a **decisional variant of the isogeny problem;**
- proof of security holds also for quantum attackers;
- it is almost as efficient as CSI-FiSh
  - same signature size,
  - public key twice as large,
  - runtime for signing and verifying is (at most) twice as slow.

How? By means of a new lossy identification protocol.

ROADMAP

1. Digital signatures and the Fiat-Shamir transform
2. What is a lossy identification protocol?
3. Our CISDH-based lossy identification protocol
4. Why a lossy identification protocol?
5. Security and efficiency of Lossy CSI-FiSh

DIGITAL SIGNATURES

A **digital signature** is composed by three PPT algorithms:

$$\mathsf{DS} = (\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$$

DIGITAL SIGNATURES

A **digital signature** is composed by three PPT algorithms:

$$DS = (\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$$

Alice runs KeyGen to generate a pair of keys: **(pk,sk)**

DIGITAL SIGNATURES

A **digital signature** is composed by three PPT algorithms:

$$\mathrm{DS} = (\mathrm{KeyGen}, \mathrm{Sign}, \mathrm{Verify})$$

Alice runs KeyGen to generate a pair of keys: **(pk,sk)**

For a message m, **Alice** runs Sign on **(sk,m)** to generate a signature σ on m

DIGITAL SIGNATURES

A **digital signature** is composed by three PPT algorithms:

$$\mathrm{DS} = (\mathrm{KeyGen}, \mathrm{Sign}, \mathrm{Verify})$$

Alice runs KeyGen to generate a pair of keys: **(pk,sk)**

For a message m, **Alice** runs Sign on **(sk,m)** to generate a signature σ on m

Any **Bob** runs Verify on $(\mathrm{pk}, \sigma, \mathrm{m})$ to verify validity of σ

DIGITAL SIGNATURES

A **digital signature** is composed by three PPT algorithms:

$$\text{DS} = (\text{KeyGen}, \text{Sign}, \text{Verify})$$

Alice runs KeyGen to generate a pair of keys: **(pk,sk)**

For a message m, **Alice** runs Sign on **(sk,m)** to generate a signature σ on m

Any **Bob** runs Verify on $(\text{pk}, \sigma, \text{m})$ to verify validity of σ

The digital signature DS is **secure** if **an attacker knowing pk (but not sk)** has **negligible success probability** in producing a pair (σ^*, m^*) s.t.

$$\text{Verify}(\text{pk}, \sigma^*, \text{m}^*) = 1$$

FIAT-SHAMIR TRANSFORM

Constructing secure and efficient digital signatures is complicated.

FIAT-SHAMIR TRANSFORM

Constructing secure and efficient digital signatures is complicated.

The **Fiat-Shamir transform**:

- turns a **secure identification protocol** into a **secure digital signature**
- it leads to **efficient signature** schemes

FIAT-SHAMIR TRANSFORM

Constructing secure and efficient digital signatures is complicated.

The **Fiat-Shamir transform**:

- turns a **secure identification protocol** into a **secure digital signature**
- it leads to **efficient signature** schemes

It has been widely used since its introduction (Crypto 1986)

ROADMAP

1. Digital signatures and the Fiat-Shamir transform ✓

2. What is a lossy identification protocol?

3. Our CISDH-based lossy identification protocol

4. Why a lossy identification protocol?

5. Security and efficiency of Lossy CSI-FiSh

WHAT IS AN IDENTIFICATION PROTOCOL?

Let $\mathscr{R} \subset X \times Y$ be a binary relation. An identification protocol

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

for $\mathscr{R}$ is a **three-move interactive protocol** between a **prover** and a **verifier**.

WHAT IS AN IDENTIFICATION PROTOCOL?

Let $\mathscr{R} \subset X \times Y$ be a binary relation. An identification protocol

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

for $\mathscr{R}$ is a **three-move interactive protocol** between a **prover** and a **verifier**.

The prover holds a public key - secret key pair (pk,sk) $\in \mathscr{R}$,

and wants to prove to the verier they know sk, without revealing sk

WHAT IS AN IDENTIFICATION PROTOCOL?

Let $\mathscr{R} \subset X \times Y$ be a binary relation. An identification protocol

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

for $\mathscr{R}$ is a **three-move interactive protocol** between a **prover** and a **verifier**.

The prover holds a public key - secret key pair (pk,sk) $\in \mathscr{R}$,

and wants to **prove** to the verier **they know sk**, without revealing sk

Prover

Verifier

WHAT IS AN IDENTIFICATION PROTOCOL?

Let $\mathscr{R} \subset X \times Y$ be a binary relation. An identification protocol

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

for $\mathscr{R}$ is a **three-move interactive protocol** between a **prover** and a **verifier**.

The prover holds a public key - secret key pair (pk,sk) $\in \mathscr{R}$,
and wants to **prove** to the verier **they know sk**, without revealing sk

Prover | **Verifier**

$\mathsf{com} \leftarrow \mathsf{P}_1(\mathsf{pk}, \mathsf{sk})$ $\xrightarrow{\mathsf{com}}$

WHAT IS AN IDENTIFICATION PROTOCOL?

Let $\mathscr{R} \subset X \times Y$ be a binary relation. An identification protocol

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

for $\mathscr{R}$ is a **three-move interactive protocol** between a **prover** and a **verifier**.

The prover holds a public key - secret key pair (pk,sk) $\in \mathscr{R}$,

and wants to prove to the verier they know sk, without revealing sk

Prover		**Verifier**
$\mathsf{com} \leftarrow \mathsf{P}_1(\mathsf{pk}, \mathsf{sk})$	$\xrightarrow{\mathsf{com}}$	
	$\xleftarrow{\mathsf{ch}}$	$\mathsf{ch} \leftarrow \mathsf{ChSet}$

WHAT IS AN IDENTIFICATION PROTOCOL?

Let $\mathscr{R} \subset X \times Y$ be a binary relation. An identification protocol

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

for $\mathscr{R}$ is a **three-move interactive protocol** between a **prover** and a **verifier**.

> The prover holds a public key - secret key pair (pk,sk) $\in \mathscr{R}$,
>
> and wants to **prove** to the verier **they know sk**, without revealing sk

Prover		**Verifier**
$\mathsf{com} \leftarrow \mathsf{P}_1(\mathsf{pk}, \mathsf{sk})$	$\xrightarrow{\mathsf{com}}$	
	$\xleftarrow{\mathsf{ch}}$	$\mathsf{ch} \leftarrow \mathsf{ChSet}$
$\mathsf{resp} \leftarrow \mathsf{P}_2(\mathsf{pk}, \mathsf{sk}, \mathsf{com}, \mathsf{ch})$	$\xrightarrow{\mathsf{resp}}$	

WHAT IS AN IDENTIFICATION PROTOCOL?

Let $\mathscr{R} \subset X \times Y$ be a binary relation. An identification protocol

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

for $\mathscr{R}$ is a **three-move interactive protocol** between a **prover** and a **verifier**.

> The prover holds a public key - secret key pair (pk,sk) $\in \mathscr{R}$,
>
> and wants to **prove** to the verier **they know sk**, without revealing sk

Prover		**Verifier**
$\mathsf{com} \leftarrow \mathsf{P}_1(\mathsf{pk}, \mathsf{sk})$	$\xrightarrow{\mathsf{com}}$	
	$\xleftarrow{\mathsf{ch}}$	$\mathsf{ch} \leftarrow \mathsf{ChSet}$
$\mathsf{resp} \leftarrow \mathsf{P}_2(\mathsf{pk}, \mathsf{sk}, \mathsf{com}, \mathsf{ch})$	$\xrightarrow{\mathsf{resp}}$	
	$\xleftarrow{1/0}$	$1/0 \leftarrow \mathsf{V}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}, \mathsf{resp})$

WHAT IS AN IDENTIFICATION PROTOCOL?

Let $\mathscr{R} \subset X \times Y$ be a binary relation. An identification protocol

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

for $\mathscr{R}$ is a **three-move interactive protocol** between a **prover** and a **verifier**.

Required properties

- Correctness
- Honest-Verifier Zero-Knowledge
- High Min-Entropy
- Perfect Unique Response
- 2-Special Soundness

WHAT IS A LOSSY IDENTIFICATION PROTOCOL?

Let $\mathscr{R} \subset X \times Y$ be a binary relation. A lossy identification protocol

$$\mathrm{ID} = (\mathrm{IGen}, \mathtt{LossyIgen}, \ \mathsf{P} = (\mathsf{P}_1, \mathsf{P}_2), \mathsf{V})$$

for $\mathscr{R}$ is a **three-move interactive protocol** between a **prover** (holding a public key-secret key pair (pk,sk) $\in \mathscr{R}$) and a **verifier**.

Required properties

- Correctness
- Honest-Verifier Zero-Knowledge
- High Min-Entropy
- Perfect Unique Response
- 2-Special Soundness

WHAT IS A LOSSY IDENTIFICATION PROTOCOL?

Let $\mathscr{R} \subset X \times Y$ be a binary relation. A lossy identification protocol

$$\mathrm{ID} = (\mathrm{IGen}, \mathrm{LossyIgen}, \ \mathrm{P} = (\mathrm{P}_1, \mathrm{P}_2), \mathrm{V})$$

for $\mathscr{R}$ is a **three-move interactive protocol** between a **prover** (holding a public key-secret key pair (pk,sk) $\in \mathscr{R}$) and a **verifier**.

Required properties

- Correctness
- Honest-Verifier Zero-Knowledge
- High Min-Entropy
- Perfect Unique Response
- Statistical Lossy Soundness

WHAT IS A LOSSY IDENTIFICATION PROTOCOL?

Let $\mathscr{R} \subset X \times Y$ be a binary relation. A lossy identification protocol

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

for $\mathscr{R}$ is a **three-move interactive protocol** between a **prover** (holding a public key-secret key pair (pk,sk) $\in \mathscr{R}$) and a **verifier**.

Required properties

- Correctness
- Honest-Verifier Zero-Knowledge
- High Min-Entropy
- Perfect Unique Response
- Statistical Lossy Soundness $\rightarrow$ An **unbounded** adversary $\mathscr{A}$ produces a **valid transcript** for $\mathrm{pk}_{\mathrm{ls}}$ with probability ϵ_{ls}.

WHAT IS A LOSSY IDENTIFICATION PROTOCOL?

Let $\mathscr{R} \subset X \times Y$ be a binary relation. A lossy identification protocol

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

for $\mathscr{R}$ is a **three-move interactive protocol** between a **prover** (holding a statement-witness pair (X,W) $\in \mathscr{R}$) and a **verifier**.

Required properties

- Correctness
- Honest-Verifier Zero-Knowledge
- High Min-Entropy
- Perfect Unique Response
- Statistical Lossy Soundness
- Indistinguishability of Lossy Statements

$$(\mathsf{pk}_{ls}, \cdot\,) \leftarrow \mathsf{LossyIgen}(1^{\lambda})$$

$\mathsf{Adv}^{\mathsf{lossy}}_{\mathscr{B}}(\lambda)$ in distinguishing real and lossy public keys is **negligible**

ROADMAP

1. Digital signatures and the Fiat-Shamir transform ✓
2. What is a lossy identification protocol? ✓
3. Our CISDH-based lossy identification protocol
4. Why a lossy identification protocol?
5. Security and efficiency of Lossy CSI-FiSh

THE CSIDH SETTING

- G finite abelian group
- X finite set

G acts **freely** and **transitively** on X

$$\begin{aligned} \star : G \times X &\to X \\ (g, \mathsf{X}) &\mapsto g \star \mathsf{X} \end{aligned}$$

- $1_G \star \mathsf{X} = \mathsf{X}$;
- $g_1 \star (g_2 \star \mathsf{X}) = g_1 g_2 \star \mathsf{X}$
- $g \mapsto g \star \mathsf{X}$ is a **bijection**

THE CSIDH SETTING

- G finite abelian group
- X finite set

G acts **freely** and **transitively** on X

$$\star : G \times X \to X$$
$$(g, \mathsf{X}) \mapsto g \star \mathsf{X}$$

- $1_G \star \mathsf{X} = \mathsf{X}$;
- $g_1 \star (g_2 \star \mathsf{X}) = g_1 g_2 \star \mathsf{X}$
- $g \mapsto g \star \mathsf{X}$ is a **bijection**

GAIP
- hard to compute g given $g \star \mathsf{X}$

THE CSIDH SETTING

- G finite abelian group
- X finite set

G is determined by a big prime p

G acts **freely** and **transitively** on X

$$\star : G \times X \to X$$
$$(g, \mathsf{X}) \mapsto g \star \mathsf{X}$$

- $1_G \star \mathsf{X} = \mathsf{X}$;
- $g_1 \star (g_2 \star \mathsf{X}) = g_1 g_2 \star \mathsf{X}$
- $g \mapsto g \star \mathsf{X}$ is a **bijection**

GAIP

- hard to compute g given $g \star \mathsf{X}$

THE CSIDH SETTING

- G finite abelian group →
- X finite set

Ideal class group $Cl(\mathcal{O})$ with $\mathcal{O} \subset \mathbb{Q}(\sqrt{-p})$

G is determined by a big prime p

G acts **freely** and **transitively** on X

$$\star : G \times X \to X$$
$$(g, \mathrm{X}) \mapsto g \star \mathrm{X}$$

- $1_G \star \mathrm{X} = \mathrm{X}$;
- $g_1 \star (g_2 \star \mathrm{X}) = g_1 g_2 \star \mathrm{X}$
- $g \mapsto g \star \mathrm{X}$ is a **bijection**

GAIP

- hard to compute g given $g \star \mathrm{X}$

THE CSIDH SETTING

- G finite abelian group $\rightarrow$
- X finite set

Ideal class group $Cl(\mathcal{O})$ with $\mathcal{O} \subset \mathbb{Q}(\sqrt{-p})$

X is the set of supersingular elliptic curves $E/\mathbb{F}_p$ s.t. $\mathrm{End}_p(E) \simeq \mathcal{O}$

G is determined by a big prime p

G acts **freely** and **transitively** on X

$$\star : G \times X \rightarrow X$$
$$(g, \mathrm{X}) \mapsto g \star \mathrm{X}$$

- $1_G \star \mathrm{X} = \mathrm{X}$;
- $g_1 \star (g_2 \star \mathrm{X}) = g_1 g_2 \star \mathrm{X}$
- $g \mapsto g \star \mathrm{X}$ is a **bijection**

GAIP
- hard to compute g given $g \star \mathrm{X}$

THE CSIDH SETTING

- G finite abelian group $\longrightarrow$
- X finite set

Ideal class group $Cl(\mathcal{O})$ with $\mathcal{O} \subset \mathbb{Q}(\sqrt{-p})$

X is the set of supersingular elliptic curves $E/\mathbb{F}_p$ s.t. $\mathrm{End}_p(E) \simeq \mathcal{O}$

G is determined by a big prime p

G acts **freely** and **transitively** on X

$$\star : G \times X \to X$$
$$(g, \mathrm{X}) \mapsto g \star \mathrm{X}$$

- $1_G \star \mathrm{X} = \mathrm{X}$;
- $g_1 \star (g_2 \star \mathrm{X}) = g_1 g_2 \star \mathrm{X}$
- $g \mapsto g \star \mathrm{X}$ is a **bijection**

GAIP
- hard to compute g given $g \star \mathrm{X}$

Fundamental assumption: $G = \langle \mathfrak{g} \rangle$, with known cardinality N (CSIDH-512 and CSI-FISH)

THE CSIDH SETTING

- G finite abelian group → Ideal class group $Cl(\mathcal{O})$ with $\mathcal{O} \subset \mathbb{Q}(\sqrt{-p})$
- X finite set

↓

X is the set of supersingular elliptic curves $E/\mathbb{F}_p$ s.t. $\mathrm{End}_p(E) \simeq \mathcal{O}$

G is determined by a big prime p

G acts **freely** and **transitively** on X

$$\star : G \times X \to X$$
$$(g, \mathrm{X}) \mapsto g \star \mathrm{X}$$

- $1_G \star \mathrm{X} = \mathrm{X}$;
- $g_1 \star (g_2 \star \mathrm{X}) = g_1 g_2 \star \mathrm{X}$
- $g \mapsto g \star \mathrm{X}$ is a **bijection**

GAIP
- hard to compute g given $g \star \mathrm{X}$

Fundamental assumption: $G = \langle \mathfrak{g} \rangle$, with known cardinality N (CSIDH-512 and CSI-FISH)

Computing **class numbers** of quadratic orders requires **subexponential complexity.**

CSI-FiSh performed a **(record) class group computation**

THE CSIDH SETTING

- G finite abelian group → Ideal class group $Cl(\mathcal{O})$ with $\mathcal{O} \subset \mathbb{Q}(\sqrt{-p})$
- X finite set

↓

X is the set of supersingular elliptic curves $E/\mathbb{F}_p$ s.t. $\mathrm{End}_p(E) \simeq \mathcal{O}$

G is determined by a big prime p

G acts **freely** and **transitively** on X

$$\star : G \times X \to X$$
$$(g, \mathrm{X}) \mapsto g \star \mathrm{X}$$

- $1_G \star \mathrm{X} = \mathrm{X}$;
- $g_1 \star (g_2 \star \mathrm{X}) = g_1 g_2 \star \mathrm{X}$
- $g \mapsto g \star \mathrm{X}$ is a **bijection**

GAIP
- hard to compute g given $g \star \mathrm{X}$

Fundamental assumption: $G = \langle \mathfrak{g} \rangle$, with known cardinality N (CSIDH-512 and CSI-FISH)

Decisional CSIDH (D-CSIDH) problem - distinguish between the distributions

$$(E, H, \mathfrak{g}^a \star E, \mathfrak{g}^a \star H) \text{ and } (E, H, E', H')$$

where $E, H, E', H' \leftarrow X, a \leftarrow \mathbb{Z}_N$.

CSI-FISH ID

$\mathsf{pp} = (p, \mathfrak{g}, N, E_0 \in X)$

CSI-FISH ID

$\mathsf{pp} = (p, \mathfrak{g}, N, E_0 \in X)$

$\mathscr{R}_{\mathsf{CSI-FiSh}} = \{(E, a) \,|\, E = \mathfrak{g}^a \star E_0\}$

CSI-FISH ID

$\mathsf{pp} = (p, \mathfrak{g}, N, E_0 \in X)$

$\mathscr{R}_{\mathsf{CSI-FiSh}} = \{(E, a) \mid E = \mathfrak{g}^a \star E_0\}$

Prover **Verifier**

CSI-FISH ID

$\mathsf{pp} = (p, \mathfrak{g}, N, E_0 \in X)$

$\mathscr{R}_{\mathsf{CSI-FiSh}} = \{(E, a) \mid E = \mathfrak{g}^a \star E_0\}$

$$E_0 \xrightarrow{\mathfrak{g}^a} E$$

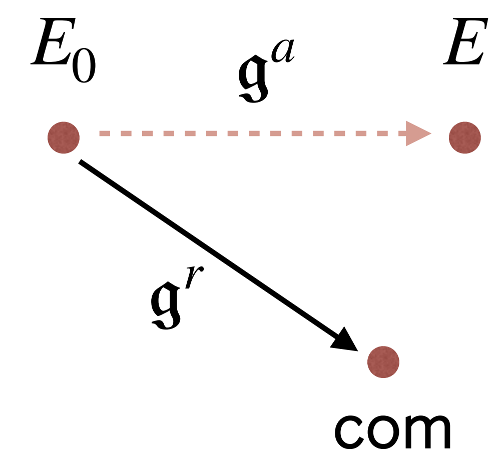
Prover

Verifier

CSI-FISH ID

$\mathsf{pp} = (p, \mathfrak{g}, N, E_0 \in X)$

$\mathscr{R}_{\mathsf{CSI-FiSh}} = \{(E, a) \mid E = \mathfrak{g}^a \star E_0\}$

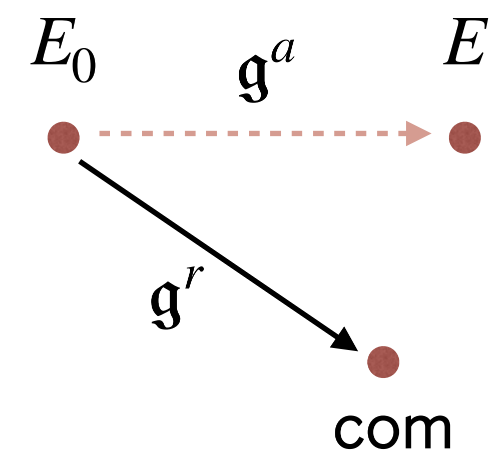


Prover		**Verifier**
$r \leftarrow \mathbb{Z}_N$, $\mathsf{com} := \mathfrak{g}^r \star E_0$	$\xrightarrow{\mathsf{com}}$

CSI-FISH ID

$\mathsf{pp} = (p, \mathfrak{g}, N, E_0 \in X)$

$\mathscr{R}_{\mathsf{CSI-FiSh}} = \{(E, a) \mid E = \mathfrak{g}^a \star E_0\}$



Prover

Verifier

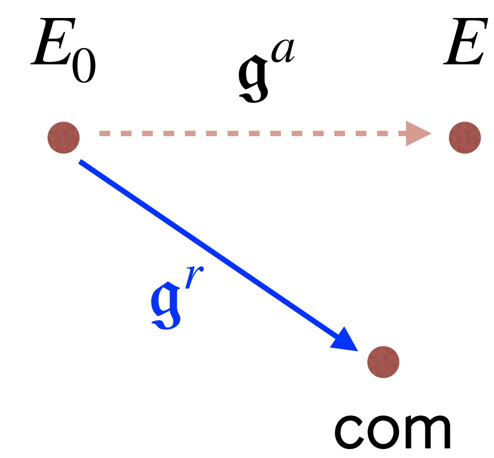
$r \leftarrow \mathbb{Z}_N$, $\mathsf{com} := \mathfrak{g}^r \star E_0$ $\xrightarrow{\mathsf{com}}$

$\xleftarrow{\mathsf{ch}}$ $\mathsf{ch} \leftarrow \{0,1\}$

CSI-FISH ID

$\mathsf{pp} = (p, \mathfrak{g}, N, E_0 \in X)$

$\mathscr{R}_{\mathsf{CSI-FiSh}} = \{(E, a) \,|\, E = \mathfrak{g}^a \star E_0\}$



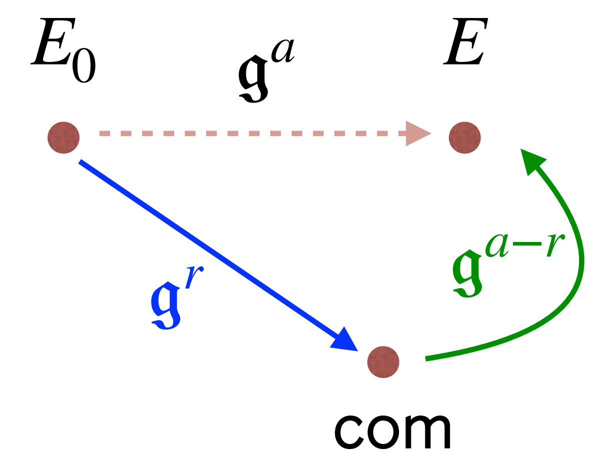
Prover		**Verifier**
$r \leftarrow \mathbb{Z}_N$, com $:= \mathfrak{g}^r \star E_0$	$\xrightarrow{\text{com}}$	
	$\xleftarrow{\text{ch}}$	ch $\leftarrow \{0,1\}$

(ch $= 0$) resp $:= r$,

CSI-FISH ID

pp $= (p, \mathfrak{g}, N, E_0 \in X)$

$\mathcal{R}_{\text{CSI-FiSh}} = \{(E, a) \mid E = \mathfrak{g}^a \star E_0\}$

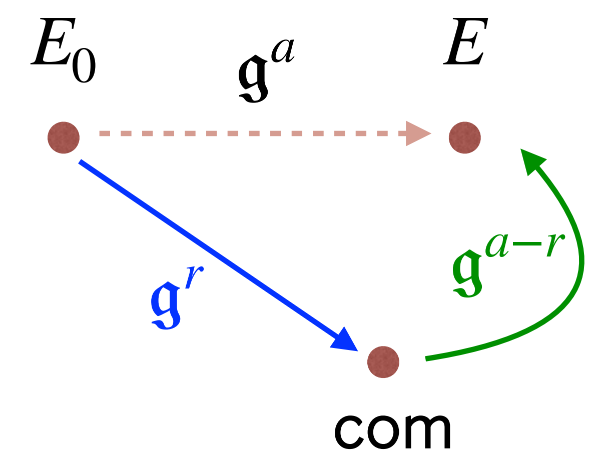


Prover		**Verifier**
$r \leftarrow \mathbb{Z}_N$, com $:= \mathfrak{g}^r \star E_0$	$\xrightarrow{\text{com}}$	
	$\xleftarrow{\text{ch}}$	ch $\leftarrow \{0,1\}$
(ch $= 0$) resp $:= r$, (ch $= 1$) resp $:= a - r$	$\xrightarrow{\text{resp}}$	

CSI-FISH ID

$\mathsf{pp} = (p, \mathfrak{g}, N, E_0 \in X)$

$\mathscr{R}_{\mathsf{CSI-FiSh}} = \{(E, a) \,|\, E = \mathfrak{g}^a \star E_0\}$



Prover | **Verifier**

$r \leftarrow \mathbb{Z}_N$, com $:= \mathfrak{g}^r \star E_0$ $\xrightarrow{\text{com}}$

$\xleftarrow{\text{ch}}$ ch $\leftarrow \{0,1\}$

(ch = 0) resp $:= r$, (ch = 1) resp $:= a - r$ $\xrightarrow{\text{resp}}$

$\xleftarrow{1/0}$

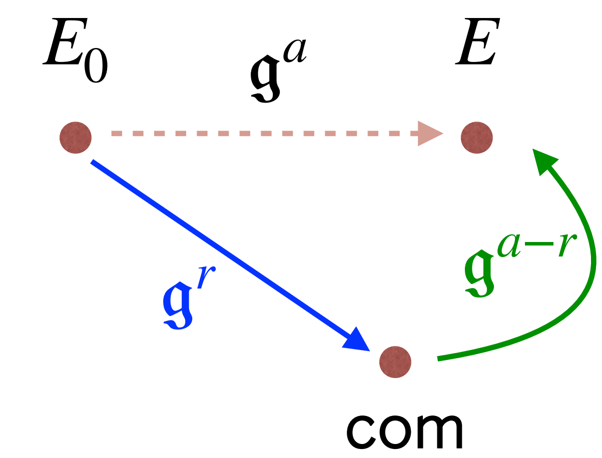
(ch = 0) com $= = \mathfrak{g}^{\text{resp}} \star E_0$

(ch = 1) $E = = \mathfrak{g}^{\text{resp}} \star$ com

OUR LOSSY ID

$\mathsf{pp} = (p, \mathfrak{g}, N, E_0 \in X)$

$$\mathscr{R}_{\text{Lossy CSI-FiSh}} = \{((E_1^{(0)}, E_2^{(0)}, E_1^{(1)}, E_2^{(1)}), a) \mid E_i^{(1)} = \mathfrak{g}^a \star E_i^{(0)},\ i = 1,2\}$$



Prover | **Verifier**

$r \leftarrow \mathbb{Z}_N$, $\mathsf{com} := \mathfrak{g}^r \star E_0$ $\xrightarrow{\text{com}}$

$\xleftarrow{\text{ch}}$ $\mathsf{ch} \leftarrow \{0,1\}$

$(\mathsf{ch} = 0)\ \mathsf{resp} := r$, $(\mathsf{ch} = 1)\ \mathsf{resp} := a - r$ $\xrightarrow{\text{resp}}$

$\xleftarrow{1/0}$

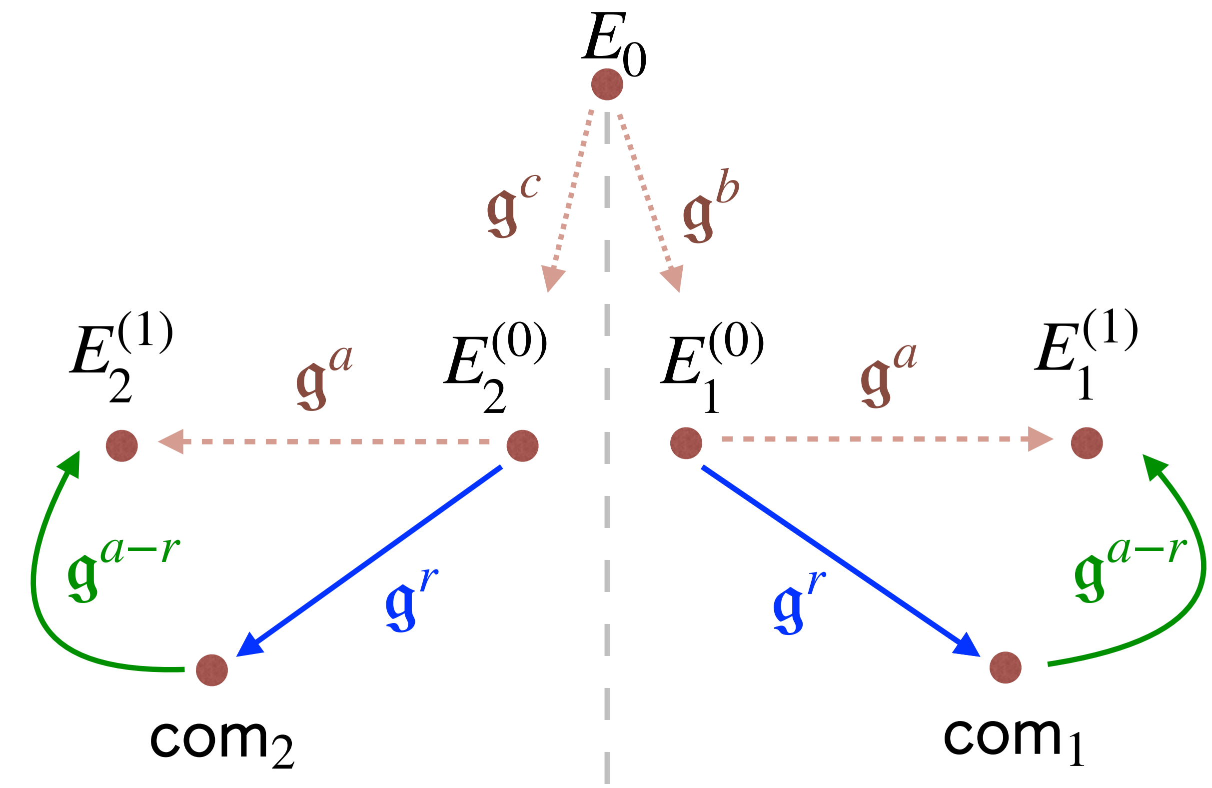
$(\mathsf{ch} = 0)\ \mathsf{com} == \mathfrak{g}^{\mathsf{resp}} \star E_0$

$(\mathsf{ch} = 1)\ E == \mathfrak{g}^{\mathsf{resp}} \star \mathsf{com}$

OUR LOSSY ID

$\mathsf{pp} = (p, \mathfrak{g}, N, E_0 \in X)$

$\mathscr{R}_{\text{Lossy CSI-FiSh}} = \{((E_1^{(0)}, E_2^{(0)}, E_1^{(1)}, E_2^{(1)}), a) \mid$
$E_i^{(1)} = \mathfrak{g}^a \star E_i^{(0)},\ i = 1,2\}$



Prover | **Verifier**

$r \leftarrow \mathbb{Z}_N$, $\mathsf{com} := \mathfrak{g}^r \star E_0$ $\xrightarrow{\mathsf{com}}$

$\xleftarrow{\mathsf{ch}}$ $\mathsf{ch} \leftarrow \{0,1\}$

$(\mathsf{ch} = 0)\ \mathsf{resp} := r$, $(\mathsf{ch} = 1)\ \mathsf{resp} := a - r$ $\xrightarrow{\mathsf{resp}}$

$\xleftarrow{1/0}$

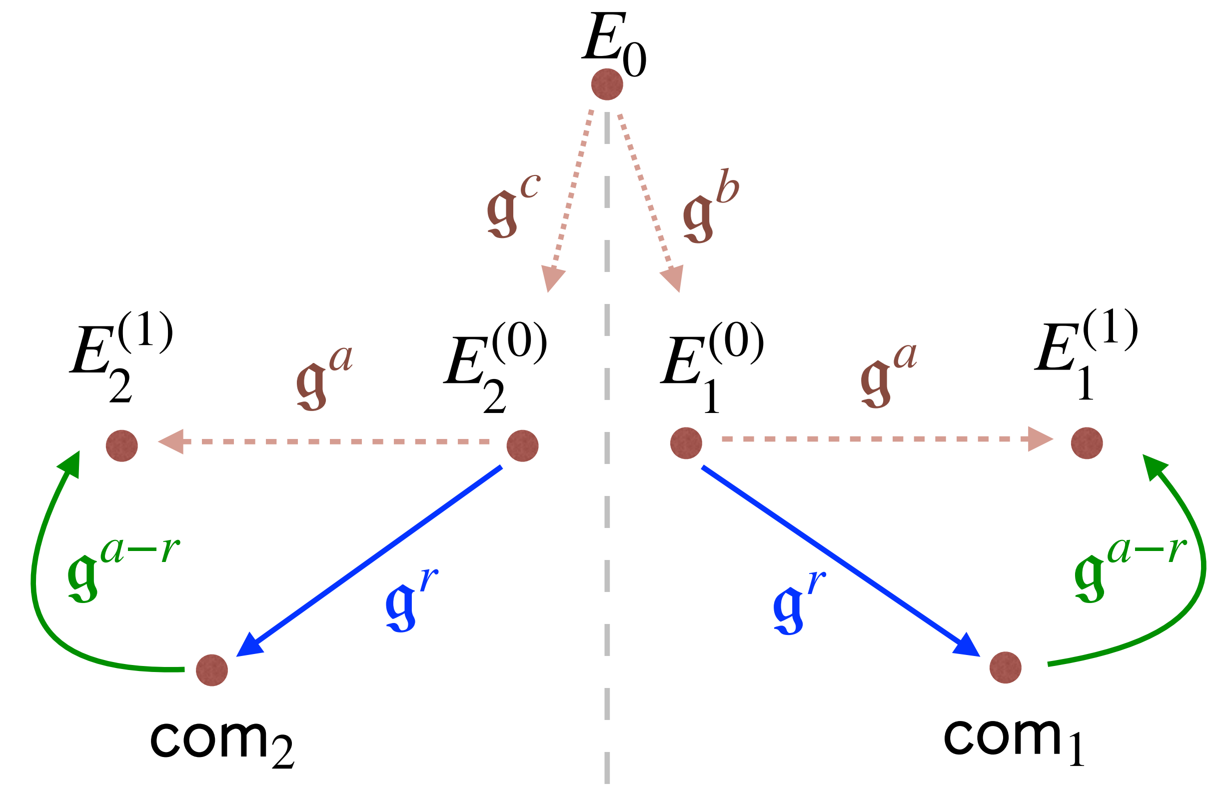
$(\mathsf{ch} = 0)\ \mathsf{com} == \mathfrak{g}^{\mathsf{resp}} \star E_0$

$(\mathsf{ch} = 1)\ E == \mathfrak{g}^{\mathsf{resp}} \star \mathsf{com}$

OUR LOSSY ID

$\mathsf{pp} = (p, \mathfrak{g}, N, E_0 \in X)$

$\mathscr{R}_{\text{Lossy CSI-FiSh}} = \{((E_1^{(0)}, E_2^{(0)}, E_1^{(1)}, E_2^{(1)}), a) \mid$
$E_i^{(1)} = \mathfrak{g}^a \star E_i^{(0)},\ i = 1,2\}$



Prover | **Verifier**

$r \leftarrow \mathbb{Z}_N,\ \mathsf{com}_i = \mathfrak{g}^r \star E_0^{(i)}$

$\xrightarrow{\mathsf{com} = (\mathsf{com}_1, \mathsf{com}_2)}$

$\mathsf{ch} \leftarrow \{0,1\}$

$\xleftarrow{\mathsf{ch}}$

$(\mathsf{ch} = 0)\ \mathsf{resp} := r,\ (\mathsf{ch} = 1)\ \mathsf{resp} := a - r$

$\xrightarrow{\mathsf{resp}}$

$\xleftarrow{1/0}$

$(\mathsf{ch} = 0)\ \ \mathsf{com}_i == \mathfrak{g}^{\mathsf{resp}} \star E_i^{(0)}$

$(\mathsf{ch} = 1)\ \ E_i^{(1)} == \mathfrak{g}^{\mathsf{resp}} \star \mathsf{com}_i$

OUR LOSSY ID

Properties

- Correctness
- Honest-Verifier Zero-Knowledge
- High Min-Entropy
- Perfect Unique Response

OUR LOSSY ID

Properties

- Correctness
- Honest-Verifier Zero-Knowledge
- High Min-Entropy
- Perfect Unique Response
- Statistical Lossy Soundness

OUR LOSSY ID

Properties

- Correctness
- Honest-Verifier Zero-Knowledge
- High Min-Entropy
- Perfect Unique Response
- Statistical Lossy Soundness →

An **unbounded** adversary $\mathscr{A}$ produces a **valid transcript** for $\mathsf{pk}_{\mathsf{ls}}$ with probability ϵ_{ls}.

$$\epsilon_{\mathsf{ls}} = \frac{1}{2} + \frac{1}{2N}$$

OUR LOSSY ID

Properties

- Correctness
- Honest-Verifier Zero-Knowledge
- High Min-Entropy
- Perfect Unique Response
- Statistical Lossy Soundness ($\epsilon_{\mathsf{ls}} = 1/2 + 1/2N$)
- Indistinguishability of Lossy Statements

$$\downarrow$$

$(\mathsf{pk}_{\mathsf{ls}}, \cdot\,) \leftarrow \mathsf{LossyIgen}(1^\lambda)$

$\mathsf{Adv}^{\mathsf{lossy}}_{\mathscr{B}}(\lambda)$ in distinguishing real and lossy public keys is **negligible**.

OUR LOSSY ID

Properties

- Correctness
- Honest-Verifier Zero-Knowledge
- High Min-Entropy
- Perfect Unique Response
- Statistical Lossy Soundness ($\epsilon_{\mathsf{ls}} = 1/2 + 1/2N$)
- Indistinguishability of Lossy Statements

↓

$$(\mathsf{pk}_{\mathsf{ls}}, \cdot\,) \leftarrow \mathsf{LossyIgen}(1^{\lambda})$$

$\mathsf{Adv}^{\mathsf{lossy}}_{\mathscr{B}}(\lambda)$ in distinguishing real and lossy public keys is **negligible**.

Real public key: $(E_1^{(0)} = \mathfrak{g}^b \star E_0, E_2^{(0)} = \mathfrak{g}^c \star E_0, \mathfrak{g}^a \star E_1^{(0)}, \mathfrak{g}^a \star E_2^{(0)})$

OUR LOSSY ID

Properties

- Correctness
- Honest-Verifier Zero-Knowledge
- High Min-Entropy
- Perfect Unique Response
- Statistical Lossy Soundness ($\epsilon_{\mathsf{ls}} = 1/2 + 1/2N$)
- Indistinguishability of Lossy Statements

$\downarrow$

$$(\mathsf{pk}_{\mathsf{ls}}, \cdot\,) \leftarrow \mathsf{LossyIgen}(1^{\lambda})$$

$\mathsf{Adv}^{\mathsf{lossy}}_{\mathscr{B}}(\lambda)$ in distinguishing real and lossy public keys is **negligible**.

Real public key: $(E_1^{(0)} = \mathfrak{g}^b \star E_0, E_2^{(0)} = \mathfrak{g}^c \star E_0, \mathfrak{g}^a \star E_1^{(0)}, \mathfrak{g}^a \star E_2^{(0)})$

Lossy public key: $(E_1^{(0)} = \mathfrak{g}^b \star E_0, E_2^{(0)} = \mathfrak{g}^c \star E_0, E', H')$

OUR LOSSY ID

Properties

- Correctness
- Honest-Verifier Zero-Knowledge
- High Min-Entropy
- Perfect Unique Response
- Statistical Lossy Soundness ($\epsilon_{\mathsf{ls}} = 1/2 + 1/2N$)
- Indistinguishability of Lossy Statements

$$(\mathsf{pk}_{\mathsf{ls}}, \cdot\,) \leftarrow \mathsf{LossyIgen}(1^{\lambda})$$

$\mathsf{Adv}^{\mathsf{lossy}}_{\mathscr{B}}(\lambda)$ in distinguishing real and lossy public keys is **negligible**.

Real public key: $(E_1^{(0)} = \mathfrak{g}^b \star E_0, E_2^{(0)} = \mathfrak{g}^c \star E_0, \mathfrak{g}^a \star E_1^{(0)}, \mathfrak{g}^a \star E_2^{(0)})$

Lossy public key: $(E_1^{(0)} = \mathfrak{g}^b \star E_0, E_2^{(0)} = \mathfrak{g}^c \star E_0, E', H')$

Decisional CSIDH (D-CSIDH) problem - distinguish between the distributions

$$(E, H, \mathfrak{g}^a \star E, \mathfrak{g}^a \star H) \text{ and } (E, H, E', H')$$

where $E, H, E', H' \leftarrow X, a \leftarrow \mathbb{Z}_N$.

ROADMAP

1. Digital signatures and the Fiat-Shamir transform ✓
2. What is a lossy identification protocol? ✓
3. Our CISDH-based lossy identification protocol ✓
4. Why a lossy identification protocol?
5. Security and efficiency of Lossy CSI-FiSh

WHY A LOSSY IDENTIFICATION PROTOCOL?

<u>Theorem</u> (Kiltz, Lyubashevsky, Schaffner - 2018)

Let ID be a **lossy identification protocol** (correct, Honest-Verifier Zero-Knowledge, α bits of min-entropy, Perfect Unique Response, ϵ_{ls}-statistical lossy soundness, indistinguishability of lossy statements), then

$$\mathsf{Adv}_{\mathscr{A}}^{\mathsf{su-cma}}(\lambda) \leq \begin{cases} \mathsf{Adv}_{\mathscr{B}}^{\mathsf{lossy}}(\lambda) + (Q_H + 1) \cdot \epsilon_{\mathsf{ls}} + 2^{-\alpha+1} + \mathsf{Adv}_{\mathscr{D}}^{\mathsf{PRF}}(\lambda) & \text{(ROM)} \\ \mathsf{Adv}_{\mathscr{B}}^{\mathsf{lossy}}(\lambda) + 8(Q_H + 1)^2 \cdot \epsilon_{\mathsf{ls}} + 2^{-\alpha+1} + \mathsf{Adv}_{\mathscr{D}}^{\mathsf{PRF}}(\lambda) & \text{(QROM)} \end{cases}$$

and $\mathsf{Time}(\mathscr{B}) = \mathsf{Time}(\mathscr{D}) = \mathsf{Time}(\mathscr{A}) + Q_H \approx \mathsf{Time}(\mathscr{A})$.

ROADMAP

1. Digital signatures and the Fiat-Shamir transform ✓
2. What is a lossy identification protocol? ✓
3. Our CISDH-based lossy identification protocol ✓
4. Why a lossy identification protocol? ✓
5. Security and efficiency of Lossy CSI-FiSh

CLASSICAL SECURITY OF LOSSY-CSI-FISH

We focus on CSIDH-512 parameters.

CLASSICAL SECURITY OF LOSSY-CSI-FISH

We focus on CSIDH-512 parameters.

				Lossy CSI-FiSh		CSI-FiSh
S	t	u	$\|\sigma\|$	$\|\mathsf{pk}\|$	Bits of security	$\|\mathsf{pk}\|$
1	74	16	2405B	256B	127	64B
3	43	14	1403B	512B	126	192B
7	30	16	983B	1024B	125	448B
15	25	13	822B	2048B	124	960B
2^6-1	17	16	564B	8.2KB	122	4KB
2^8-1	14	11	468B	32.8KB	120	16.3KB
$2^{10}-1$	12	7	404B	131KB	118	65.5KB
$2^{12}-1$	10	11	339B	524KB	116	262KB
$2^{15}-1$	8	16	274B	4MB	113	2MB

QUANTUM SECURITY OF LOSSY-CSI-FISH

We focus on CSIDH-512 parameters.

			Conservative variant			Optimistic variant		
S	u	$\vert \mathsf{pk} \vert$	t	$\vert\sigma\vert$	Bits of security	t	$\vert\sigma\vert$	Bits of security
1	16	256B	64	2080B	55	74	2405B	63
3	14	512B	37	1208B	54	43	1403B	62
7	16	1024B	26	852B	53	30	983B	61
15	13	2048B	21	691B	52	25	822B	60
2^6-1	16	8.2KB	15	497B	50	17	564B	58
2^8-1	11	32.8KB	12	401B	48	14	468B	56
$2^{10}-1$	7	131KB	10	337B	46	12	404B	54
$2^{12}-1$	11	524KB	9	305B	44	10	339B	52
$2^{15}-1$	16	4MB	7	240B	41	8	274B	49

EFFICIENCY OF LOSSY-CSI-FISH

Costs are dominated by the computation of class group actions:

- **Key Generation:** $2S + 2$ (S in CSI-FiSh)
- **Signing:** $2S$ (S in CSI-FiSh)
- **Verifying:** $2S$ (S in CSI-FiSh)

Estimated running times

(S, t, u)	Key Gen	Sign	Ver
$(2^{15} - 1, 7, 16)$	56m	800ms	800ms
$(2^{3} - 1, 28, 16)$	920ms	3s	3s

Thanks for your attention

Federico Pintore
Mathematical Institute, University of Oxford

federico.pintore@maths.ox.ac.uk