# SIGNITC:
# Supersingular Isogeny Graph Non-Interactive Timed Commitments

Knud Ahrens

Faculty of Computer Science and Mathematics
University of Passau, Germany

Central European Conference on Cryptology 2025
19 June 2025

# Non-Interactive Timed Commitments

# Non-Interactive Timed Commitment[1] (NITC)

A $(t_{com}, t_{cv}, t_{dv}, t_{fd})$- *non-interactive timed commitment scheme* (NITC) is a tuple $\mathtt{TC} = (\mathtt{PGen}, \mathtt{Com}, \mathtt{ComVrfy}, \mathtt{DecVrfy}, \mathtt{FDecom})$ of five algorithms with the following behaviour:

$\mathtt{PGen}\ \ 1^\kappa \mapsto \mathbf{crs}$

$\mathtt{Com}\ \ (\mathbf{crs}, m) \mapsto (\mathbf{C}, \pi_{\mathsf{com}}, \pi_{\mathsf{dec}})$ in time at most $t_{com}$

$\mathtt{ComVrfy}\ \ (\mathbf{crs}, \mathbf{C}, \pi_{\mathsf{com}}) \mapsto (\mathbf{accept}$ or $\mathbf{reject})$ in time at most $t_{cv}$

$\mathtt{DecVrfy}\ \ (\mathbf{crs}, \mathbf{C}, m, \pi_{\mathsf{dec}}) \mapsto (\mathbf{accept}$ or $\mathbf{reject})$ in time at most $t_{dv}$

$\mathtt{FDecom}\ \ (\mathbf{crs}, \mathbf{C}) \mapsto (m$ or $\mathbf{invalid})$ in time *at least* $t_{fd}$

We require that for all $\kappa$, all $\mathbf{crs}$ output by $\mathtt{PGen}$, all $m$ and all $\mathbf{C}, \pi_{\mathsf{com}}, \pi_{\mathsf{dec}}$ output by $\mathtt{Com}(\mathbf{crs}, m)$, it holds that

$$\mathtt{ComVrfy}(\mathbf{crs}, \mathbf{C}, \pi_{\mathsf{com}}) = \mathbf{accept}, \quad \mathit{DecVrfy}(\mathbf{crs}, \mathbf{C}, m, \pi_{\mathsf{dec}}) = \mathbf{accept}, \quad \mathtt{FDecom}(\mathbf{crs}, \mathbf{C}) = m.$$

[1] Katz, Loss, and Xu [9]

# NITC Overview

$$\texttt{PGen}(1^\kappa) = \textbf{crs}$$

| Connor | | Veronica |
|---|---|---|
| $\texttt{Com}(\textbf{crs}, m) = (\mathbf{C}, \pi_{\text{com}}, \pi_{\text{dec}})$ | $\xrightarrow[(\mathbf{C}, \pi_{\text{com}})]{\text{commitment}}$ | $\texttt{ComVrfy}(\textbf{crs}, \mathbf{C}, \pi_{\text{com}}) = (\textbf{accept}$ or $\textbf{reject})$ |
| Honest | $\xrightarrow[(m, \pi_{\text{dec}})]{\text{decommitment}}$ | $\texttt{DecVrfy}(\textbf{crs}, \mathbf{C}, m, \pi_{\text{dec}}) = (\textbf{accept}$ or $\textbf{reject})$ |
| Dishonest | $\xrightarrow[\text{decommitment}]{\text{forced}}$ | $\texttt{FDecom}(\textbf{crs}, \mathbf{C}) = (m$ or $\textbf{invalid})$ |

FDecom takes at least time $t_{\text{fd}}$ (delay).

# Properties

To be relevant for applications a NITC also needs to satisfy three further properties.

**Practicality** $t_{cv}, t_{dv} \ll t_{fd}$, i.e. verification is much faster than forcefully opening the commitment.

**Hiding** The commitment does not leak information about the message (for time $t_{fd}$).

**Binding** The commitment can not be opened to two different messages.

Katz et al. [9] state that NITCs are useful for sealed bid auctions and as primitive for other cryptographic protocols.

# Example for Application

Alice and Chris want to flip a coin over the internet.

## Naive

Both send a random number and they take the sum of both numbers modulo 2.
Very fast, but easy to cheat.

# Example for Application

Alice and Chris want to flip a coin over the internet.

## Naive

Both send a random number and they take the sum of both numbers modulo 2.
Very fast, but easy to cheat.

## Verifiable Delay Function (VDF)

Both compute a VDF with their random number as input (challenge) and send the output (response).
Slow, because both have to compute a VDF, but hard to cheat.

# Example for Application

Alice and Chris want to flip a coin over the internet.

## Naive

Both send a random number and they take the sum of both numbers modulo 2.
Very fast, but easy to cheat.

## Verifiable Delay Function (VDF)

Both compute a VDF with their random number as input (challenge) and send the output (response).
Slow, because both have to compute a VDF, but hard to cheat.

## NITC

Both commit to a random number and only open their commitment once they received the other one.
Fast (if both are honest) and hard to cheat.

# Supersingular Isogeny Graphs

# Isogeny Basics

Quantum secure schemes like SQISign[2] or CSIDH[3] use isogenies between supersingular elliptic curves. They have small key sizes, but they are comparatively slow.

## Isogenies

- Isogenies $\varphi$ are homomorphisms between elliptic curves.
- They can be determined by their kernel.
- The degree of $\varphi$ is the number of points in its kernel.

[2] De Feo, Kohel, Leroux, Petit, and Wesolowski [7]
[3] Castryck, Lange, Martindale, Panny, and Renes [4]

# Isogeny Basics

Quantum secure schemes like SQISign[2] or CSIDH[3] use isogenies between supersingular elliptic curves. They have small key sizes, but they are comparatively slow.

## Isogenies

- Isogenies $\varphi$ are homomorphisms between elliptic curves.
- They can be determined by their kernel.
- The degree of $\varphi$ is the number of points in its kernel.

## Isogeny Graph

- Dual isogenies $\widehat{\varphi}$ are "reverse" maps.
- Isomorphic curves have the same $j$-invariant.
- The isogeny graph has $j$-invariants as vertices and isogenies as edges.

[2] De Feo, Kohel, Leroux, Petit, and Wesolowski [7]
[3] Castryck, Lange, Martindale, Panny, and Renes [4]

# Deuring Correspondence

Let $\mathcal{B}_{p,\infty}$ be the quaternion algebra with $\mathbb{Q}$-basis $\{1, \mathrm{i}, \mathrm{j}, \mathrm{k}\}$ and $\mathrm{i}^2 = -1$, $\mathrm{j}^2 = -p$, $\mathrm{k} = \mathrm{ij} = -\mathrm{ji}$.

## Supersingular Elliptic Curves

$E$ is *supersingular* if and only if $\operatorname{End} E$ is isomorphic to a maximal order $\mathcal{O}$ in $\mathcal{B}_{p,\infty}$.
Supersingular elliptic curves therefore have non-commutative endomorphism rings.

## Deuring Correspondence[4]

An isogeny $\varphi\colon E \to E'$ of degree $\ell$ corresponds to a left ideal $I_\varphi$ of norm $\ell$ in $\mathcal{O} \cong \operatorname{End} E$ and $\operatorname{End} E'$ is isomorphic to the right order $\mathcal{O}_R(I_\varphi) = \{\alpha \in \mathcal{B}_{p,\infty} \mid I_\varphi \alpha \subseteq I_\varphi\}$ of $I_\varphi$.

[4] Deuring [8]

# Isogeny Problems

Polynomial problems:

**Vélu** Compute isogeny $\varphi_K \colon E \to E_K \cong E/\langle K \rangle$ given its kernel $\ker \varphi = \langle K \rangle$ for $K \in E$. Complexity depends on smoothness and size of degree $\deg \varphi_K = \operatorname{ord} K$.

**KLPT** Given an ideal $I$ of a maximal order $\mathcal{O} \subset \mathcal{B}_{p,\infty}$, find an equivalent ideal such that its norm is small or a prime power.

**Deuring** Given $\mathcal{O} \cong \operatorname{End} E$, translate between isogenies $\varphi \colon E \to E'$ and the corresponding $I_\varphi$.

Hard problems[5]:

**IsogPath** Given two (isogenous) supersingular elliptic curves $E, E'$ and a prime $\ell$, find a path from $E$ to $E'$ in the $\ell$-isogeny graph.

**EndRing** Given a supersingular elliptic curve $E$, find four endomorphisms that generate $\operatorname{End} E$ (or four quaternions in $\mathcal{B}_{p,\infty}$ that generate $\mathcal{O} \cong \operatorname{End} E$) as a lattice.

[5] Wesolowski [10]

# Shortcuts

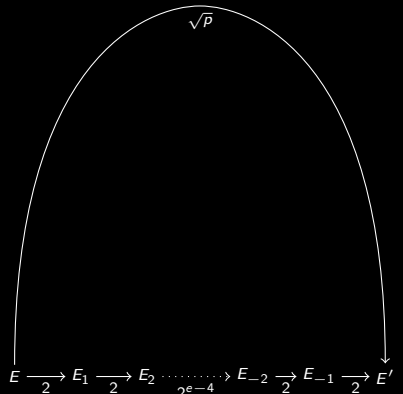

$\varphi\colon E \to E'$
Isogeny
$\deg \varphi = d$
End $E \cong \mathcal{O}$
Deuring
$I_\varphi \subset \mathcal{O}$
Ideal
$\operatorname{nrd} I_\varphi = d$
KLPT
$\widetilde{I}_\varphi \subset \mathcal{O}$
Ideal
$\operatorname{nrd} \widetilde{I}_\varphi = \widetilde{d}$
End $E \cong \mathcal{O}$
Deuring
$\widetilde{\varphi}\colon E \to E'$
Isogeny
$\deg \widetilde{\varphi} = \widetilde{d}$

# Shortcuts

$$\underset{\text{Isogeny}\\ \deg\varphi = d}{\varphi\colon E \to E'} \xrightarrow[\text{Deuring}]{\operatorname{End} E \cong \mathcal{O}} \underset{\operatorname{nrd} I_\varphi = d}{I_\varphi \subset \mathcal{O}} \xrightarrow{\text{KLPT}} \underset{\operatorname{nrd} \widetilde{I}_\varphi = \widetilde{d}}{\widetilde{I}_\varphi \subset \mathcal{O}} \xrightarrow[\text{Deuring}]{\operatorname{End} E \cong \mathcal{O}} \underset{\deg\widetilde{\varphi} = \widetilde{d}}{\widetilde{\varphi}\colon E \to E'}$$

Let $p$ be of size 256 bit. We can use KLPT in two ways:

| Type of KLPT | Size of $\widetilde{d}$ | Complexity of $\widetilde{\varphi}$ |
|---|---|---|
| $\widetilde{d}$ smooth ($\widetilde{d} = 2^e$) | $\approx p^3 \approx 2^{768}$ | $O((\log \widetilde{d})^2) \approx 2^{20}$ |
| $\widetilde{d}$ prime | $\approx \sqrt{p} \approx 2^{128}$ | $\widetilde{O}(\sqrt{\widetilde{d}}) > 2^{64}$ |



Supersingular Isogeny Graph Non-Interactive Timed Commitments
SIGNITC[6]

[6] Ahrens [1] (ia.cr/2024/1225)

# Simplified Overview

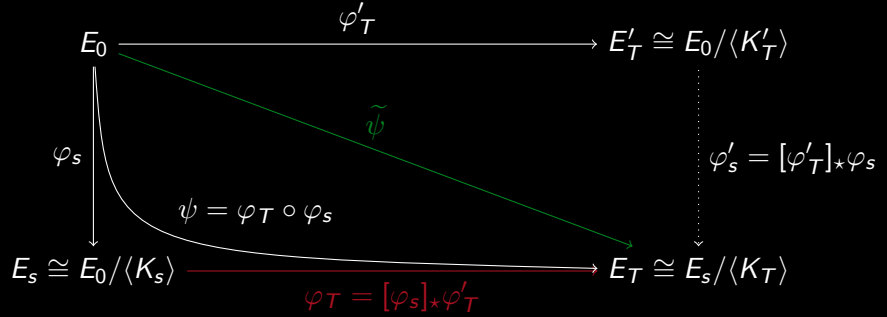
$\texttt{PGen}\ 1^\kappa \mapsto \mathbf{crs}$ = parameters and pre-computation

$\texttt{Com}\ (\mathbf{crs}, m) \mapsto (\mathbf{C}, \pi_{\mathsf{com}}, \pi_{\mathsf{dec}}) = ((E_s, K_T, u), (), (K_s, K'_T))$ $\qquad u = m \ominus F(j(E_T))$

$\texttt{ComVrfy}\ (\mathbf{crs}, \mathbf{C}, \pi_{\mathsf{com}}) \mapsto (\mathbf{accept}\ \text{or}\ \mathbf{reject})$

$\texttt{DecVrfy}\ (\mathbf{crs}, \mathbf{C}, m, \pi_{\mathsf{dec}}) \mapsto (\mathbf{accept}\ \text{or}\ \mathbf{reject})$

$\texttt{FDecom}\ (\mathbf{crs}, \mathbf{C}) \mapsto m$ $\qquad m = u \oplus F(j(E_T))$



# Simplified Overview

PGen $1^\kappa \mapsto \mathbf{crs}$ = parameters and pre-computation

Com $(\mathbf{crs}, m) \mapsto (\mathbf{C}, \pi_{\mathsf{com}}, \pi_{\mathsf{dec}}) = ((E_s, K_T, u), (), (K_s, K'_T))$

ComVrfy $(\mathbf{crs}, \mathbf{C}, \pi_{\mathsf{com}}) \mapsto$ (**accept** or **reject**)

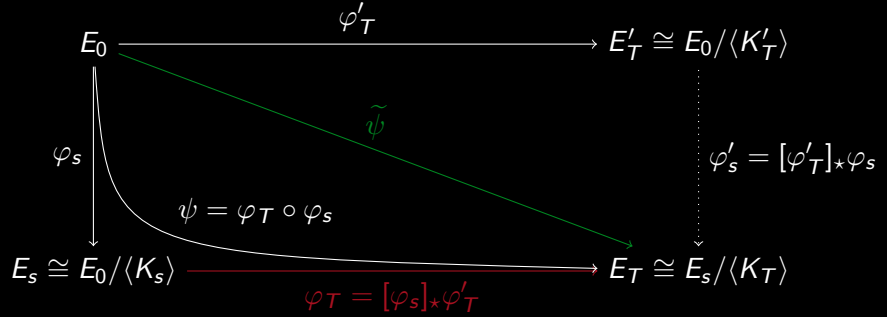
DecVrfy $(\mathbf{crs}, \mathbf{C}, m, \pi_{\mathsf{dec}}) \mapsto$ (**accept** or **reject**)

FDecom $(\mathbf{crs}, \mathbf{C}) \mapsto m$

Hiding/Binding:

$u = m \ominus F(j(E_T))$

$m = u \oplus F(j(E_T))$



# Parameter Generation Algorithm PGen

**Require:** Security parameter $1^\kappa$
**Ensure:** $\mathbf{crs} = (\mathbf{crs}_0, \mathbf{crs}_s, \mathbf{crs}_T, \mathbf{crs}_{\mathtt{ItI}})$

$\mathbf{crs}_0$ Starting curve $E_0$, message group $(M, \oplus)$, inverse resistant function $F\colon J_{SS} \to M$

$\mathbf{crs}_s$ Pre-computations for $\varphi_s$

$\mathbf{crs}_T$ Pre-computations for $\varphi_T$ (or rather $\varphi'_T$)

$\mathbf{crs}_{\mathtt{ItI}}$ Pre-computations for `IdealToIsogeny`

$J_{SS}$ is the set of supersingular $j$-invariants in $\mathbb{F}_{p^2}$.

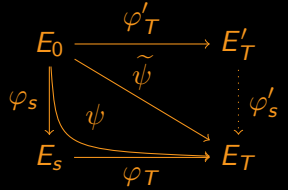
**Definition (Inverse Resistant Functions)**

A function $F\colon X \to Y$ is $\lambda$-*inverse resistant*, if for all $y \in Y$ the preimage $F^{-1}(y) \subseteq X$ has at least $2^\lambda$ elements.

# Commitment Algorithm Com

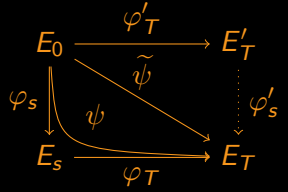
**Require:** Common reference string **crs**, message $m \in M$
**Ensure:** $(\mathbf{C}, \pi_{\text{com}}, \pi_{\text{dec}}) = \big((E_s, K_T, u), (), (K_s, K'_T)\big)$

1: Choose random isogeny $\varphi_s \colon E_0 \to E_s$ with kernel $\langle K_s \rangle$
2: Compute corresponding ideal $I_s$



# Commitment Algorithm Com

**Require:** Common reference string **crs**, message $m \in M$
**Ensure:** $(\mathbf{C}, \pi_{\text{com}}, \pi_{\text{dec}}) = \big((E_s, K_T, u), (), (K_s, K'_T)\big)$

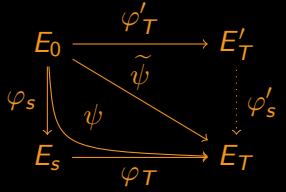



1: Choose random isogeny $\varphi_s \colon E_0 \to E_s$ with kernel $\langle K_s \rangle$
2: Compute corresponding ideal $I_s$

3: Choose random isogeny $\varphi'_T \colon E_0 \to E'_T$ with kernel $\langle K'_T \rangle$
4: Compute corresponding ideal $I'_T$
5: Compute $K_T = \varphi_s(K'_T)$ such that $\ker \varphi_T = \langle K_T \rangle$
6: Compute ideal $I_\psi = I_s \cap I'_T$ corresponding to isogeny $\psi = \varphi_T \circ \varphi_s$
7: Use `IdealToIsogeny` to get shortcut $\widetilde{\psi}$ and $\widetilde{E}_T \cong E_s/\langle K_T \rangle$ (Go back to step 3 if it fails)

# Commitment Algorithm Com

**Require:** Common reference string **crs**, message $m \in M$
**Ensure:** $(\mathbf{C}, \pi_{\text{com}}, \pi_{\text{dec}}) = \big((E_s, K_T, u), (), (K_s, K'_T)\big)$




1: Choose random isogeny $\varphi_s \colon E_0 \to E_s$ with kernel $\langle K_s \rangle$
2: Compute corresponding ideal $I_s$

3: Choose random isogeny $\varphi'_T \colon E_0 \to E'_T$ with kernel $\langle K'_T \rangle$
4: Compute corresponding ideal $I'_T$
5: Compute $K_T = \varphi_s(K'_T)$ such that $\ker \varphi_T = \langle K_T \rangle$
6: Compute ideal $I_\psi = I_s \cap I'_T$ corresponding to isogeny $\psi = \varphi_T \circ \varphi_s$
7: Use `IdealToIsogeny` to get shortcut $\widetilde{\psi}$ and $\widetilde{E}_T \cong E_s/\langle K_T \rangle$ (Go back to step 3 if it fails)

8: Compute $\widetilde{j}_T = j(\widetilde{E}_T)$ and $u = m \ominus F(\widetilde{j}_T) \in M$ ▷ $F(\widetilde{j}_T) = F(j(E_T))$
9: **return** $\big((E_s, K_T, u), (), (K_s, K'_T)\big)$

# Commitment Verification Algorithm ComVrfy

**Require:** Common reference string **crs**, commitment **C** and proof $\pi_{\text{com}}$

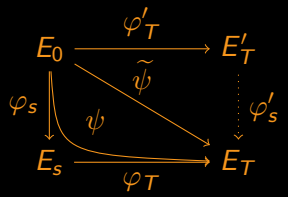
1: Check if $E_s$ is an elliptic curve over $\mathbb{F}_{p^2}$, $K_T \in E_s$ and $u \in M$
2: *Optional: check* $K_T \in \mathbb{F}_{p^{2e}}^2$ ▷ *Check upper bound for degree of* $\varphi_T$

3: **return** (**accept**/**reject**)

# Decommitment Verification Algorithm `DecVrfy`

**Require:** Common reference string **crs**, commitment **C**
**Require:** Message $m$, decommitment proof $\pi_{\text{dec}}$

1: Check $E_s \cong E_0/\langle K_s \rangle$ and $\varphi_s(K'_T) = K_T$




2: Compute an ideal $I_s$ corresponding to isogeny $\varphi_s$
3: Compute an ideal $I'_T$ corresponding to isogeny $\varphi'_T$
4: Compute ideal $I_\psi = I_s \cap I'_T$ corresponding to isogeny $\psi = \varphi_T \circ \varphi_s$
5: Use `IdealToIsogeny` to get shortcut $\widetilde{\psi}$ and $\widetilde{E}_T \cong E_s/\langle K_T \rangle$

6: Compute $\widetilde{j}_T = j(\widetilde{E}_T)$ and check $u \oplus F(\widetilde{j}_T) = m$ ▷ $F(\widetilde{j}_T) = F(j(E_T))$
7: **return** (**accept**/**reject**)

# Forced Decommitment Algorithm FDecom

**Require:** Common reference string **crs**, commitment **C**
**Ensure:** Message $m$

1: Compute $E_T \cong E_s/\langle K_T \rangle$ as codomain of $\varphi_T \colon E_s \to E_T$
2: Compute $j_T = j(E_T)$ and $m = u \oplus F(j_T)$

3: **return** $m$

# IdealToIsogeny Algorithms

| Variants | one dimensional | higher dimensional |
|---|---|---|
| Examples | SQISign[7] | SQIsign2D-West[8], SQIsignHD[9] |
| Prime | SQISign-friendly primes | $p = c2^k - 1$ with $c$ as small as possible. |
| Pre-computation | $\mathbf{crs}_{\mathtt{ItI}}$ can be empty | $\mathbf{crs}_{\mathtt{ItI}}$ contains basis of $E_0[2^k]$ |
| Pro | one dimesional isogenies | isogenies of degree $d \mid p^2 - 1$ |
| Contra | isogenies of degree $d \approx p^3$ | isogenies of higher dimension |

[7] Chavez-Saab, Corte-Real Santos, De Feo, Eriksen, Hess, Kohel, Leroux, Longa, Meyer, Panny, Patranabis, Petit, Rodríguez Henríquez, Schaeffler, and Wesolowski [5]

[8] Basso, Dartois, Feo, Leroux, Maino, Pope, Robert, and Wesolowski [2]

[9] Dartois, Leroux, Robert, and Wesolowski [6]

# Conclusion

# Conclusion

SIGNITC is a practical NITC that satisfies hiding and binding.

## Advantages

- Works purely within isogeny-based cryptography.
- Presumably quantum secure.
- Highly adjustable with (almost) arbitrary delay.
- Explicit algorithms with known efficient implementations.

## Disadvantages

- Some algorithms and topics are quite involved.
- Slightly weaker hiding and binding properties.

# References I


[1] Knud Ahrens. SIGNITC: Supersingular isogeny graph non-interactive timed commitments. Cryptology ePrint Archive, Paper 2024/1225, 2024. URL https://eprint.iacr.org/2024/1225.

[2] Andrea Basso, Pierrick Dartois, Luca De Feo, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert, and Benjamin Wesolowski. Sqisign2d–west. In Kai-Min Chung and Yu Sasaki, editors, *Advances in Cryptology – ASIACRYPT 2024*, pages 339–370, Singapore, 2025. Springer Nature Singapore. ISBN 978-981-96-0891-1. doi: 10.1007/978-981-96-0891-1_11.

[3] Daniel J. Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith. Faster computation of isogenies of large prime degree. In Steven D. Galbraith, editor, *Proceedings of the Fourteenth Algorithmic Number Theory Symposium*, pages 39–55, Berkeley, 2020. Mathematical Sciences Publishers. doi: 10.2140/obs.2020.4.39.

[4] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In Thomas Peyrin and Steven Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018*, pages 395–427, Cham, 2018. Springer International Publishing. doi: 10.1007/978-3-030-03332-3_15.

[5] Jorge Chavez-Saab, Maria Corte-Real Santos, Luca De Feo, Jonathan Komada Eriksen, Basil Hess, David Kohel, Antonin Leroux, Patrick Longa, Michael Meyer, Lorenz Panny, Sikhar Patranabis, Christophe Petit, Francisco Rodríguez Henríquez, Sina Schaeffler, and Benjamin Wesolowski. SQIsign algorithm specifications and supporting documentation. Project Homepage, 2023. URL https://sqisign.org/spec/sqisign-20230601.pdf.

# References II


[6] Pierrick Dartois, Antonin Leroux, Damien Robert, and Benjamin Wesolowski. SQIsignHD: New dimensions in cryptography. In Marc Joye and Gregor Leander, editors, *Advances in Cryptology – EUROCRYPT 2024*, pages 3–32, Cham, 2024. Springer Nature Switzerland. ISBN 978-3-031-58716-0. doi: 10.1007/978-3-031-58716-0_1.

[7] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: Compact post-quantum signatures from quaternions and isogenies. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 64–93, Cham, 2020. Springer International Publishing. doi: 10.1007/978-3-030-64837-4_3.

[8] Max Deuring. Die Typen der Multiplikatorenringe elliptischer funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941. doi: 10.1007/BF02940746.

[9] Jonathan Katz, Julian Loss, and Jiayu Xu. On the security of time-lock puzzles and timed commitments. In Rafael Pass and Krzysztof Pietrzak, editors, *Theory of Cryptography*, pages 390–413, Cham, 2020. Springer International Publishing. doi: 10.1007/978-3-030-64381-2_14.

[10] Benjamin Wesolowski. The supersingular isogeny path and endomorphism ring problems are equivalent. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1100–1111, 2022. doi: 10.1109/FOCS52979.2021.00109.

# Parameters

We choose $E_0 \colon y^2 = x^3 + x$ with $\mathcal{O}_0 = \langle 1, \mathrm{i}, \frac{\mathrm{i}+\mathrm{j}}{2}, \frac{1+\mathrm{k}}{2} \rangle_{\mathbb{Z}}$ and $p \equiv 3 \bmod 4$.

The message group is $M = \mathbb{Z}/N\mathbb{Z}$ for an integer $N \leq \lfloor p^{1/4}/12 \rfloor$.

For $J_{SS} \subset \mathbb{F}_{p^2} \cong \mathbb{F}_p[\mathrm{i}]$ we take $F \colon J_{SS} \to M = \mathbb{Z}/N\mathbb{Z}, \quad a + b\mathrm{i} \mapsto a + |b| \bmod N$.

Then we have the following:

- Membership testing and group operations in $M$ are efficient.
- $F$ can be computed efficiently.
- $F$ is sufficiently inverse resistant.

# NIST level I with $\kappa = 128$

SQIsign-friendly prime $p = p^I_{1973}$ with $\log_2 p^I_{1973} \approx 251.9$ from the specifications of SQIsign [5].

$$
\begin{aligned}
p^I_{1973} &= \texttt{0x34e29e286b95d98c33a6a86587407437252c9e49355147ffffffffffffffff} \\
p^2 - 1 &= 2^{76} \cdot 3^{36} \cdot 7^4 \cdot 11 \cdot 13 \cdot 23^2 \cdot 37 \cdot 59^2 \cdot 89 \cdot 97 \cdot 101^2 \cdot 107 \cdot 109^2 \cdot 131 \cdot 137 \cdot 197^2 \cdot 223 \\
&\quad \cdot 239 \cdot 383 \cdot 389 \cdot 491^2 \cdot 499 \cdot 607 \cdot 743^2 \cdot 1033 \cdot 1049 \cdot 1193 \cdot 1913^2 \cdot 1973 \\
&\quad \cdot 32587069 \cdot 275446333 \cdot 1031359276391767 \\
d_s &= 2^{150} \\
d_T &= 7^4 \cdot 11 \cdot 13 \cdot 37 \cdot 89 \cdot 97 \cdot 107 \cdot 131 \cdot 137 \cdot 223 \cdot 239 \cdot 383 \cdot 389 \cdot 499 \cdot 607 \cdot 1033 \cdot 1049 \\
&\quad \cdot 1193 \cdot 1973 \cdot 32587069 \cdot 275446333 \quad \text{(delay of roughly 1 minute}^{10}\text{)} \\
d_T &= 1031359276391767 \quad \text{(estimated delay of roughly 1 day}^{10}\text{)}
\end{aligned}
$$

For the group $M = \mathbb{Z}/N\mathbb{Z}$ we choose $N \leq 2^{59} < 1036363420827959282$.

[10] Using Sage on an old laptop

# Security

# Computing Isogenies

Let $\varphi$ be an isogeny of prime degree $q$.

- Vélu's formulae compute $\varphi$ in time $O(q)$.
- The $\sqrt{\text{élu}}$ algorithm[11] computes $\varphi$ in time $O(\sqrt{q})$.
- The crossover point for optimised algorithms is at $q \approx 100$.

**Assumption (Isogeny Computation Assumption)**

*Given a supersingular elliptic curve $E$ and a point $K$ of order $d$ on $E$. Let $\varphi$ be the isogeny with kernel $\langle K \rangle$ and $d = \prod p_i^{e_i}$ the prime factorization of $d$. Computing the codomain $E/\langle K \rangle$ of $\varphi$ takes time $\Theta\big(\sum_{p_i<100} e_i p_i + \sum_{p_i>100} e_i \sqrt{p_i}\big)$.*

[11] Bernstein, De Feo, Leroux, and Smith [3]

# Practical NITC

SIGNITC is a NITC scheme:

- All algorithms have the correct input and output arguments.
- For all $\kappa$ and $m \in M$, every set of honestly generated $(\kappa, m, \mathbf{crs}, \mathbf{C}, \pi_{\mathsf{com}}, \pi_{\mathsf{dec}})$ satisfies verification $\texttt{ComVrfy}(\mathbf{crs}, \mathbf{C}, \pi_{\mathsf{com}}) = \mathbf{accept} = \texttt{DecVrfy}(\mathbf{crs}, \mathbf{C}, m, \pi_{\mathsf{dec}})$ and forced decommitment $\texttt{FDecom}(\mathbf{crs}, \mathbf{C}) = m$.

SIGNITC is a practical NITC:

- The subroutines used in `Com` and `DecVrfy` take time poly($\log p$).
- The degree $d_T$ of the long isogeny $\varphi_T$ can be made almost arbitrarily large / non-smooth.
- We can choose $d_T$ such that $t_{com}, t_{cv}, t_{dv} \ll t_{fd}$.

# Hiding

The pre-computation phase can only provide a negligible advantage for an adversary $\mathcal{A}$.

In the online phase $\mathcal{A}$ outputs two messages $m_0, m_1$ and receives the output $\mathbf{C}_b = (E_s, K_T, u_b)$ of $\mathtt{Com}(\mathbf{crs}, m_b)$ for a uniform $b \in \{0, 1\}$.

## Proof sketch

- $F(j_T)$ is either $F_0 = \ominus u_b \oplus m_0$ or $F_1 = \ominus u_b \oplus m_1$.
- Since $F$ is inverse resistant, the advantage over guessing is negligible.
- Therefore $\mathcal{A}$ has to compute $j_T = j(E_T)$ in order to find the correct $b' = b$.
- This is as slow as $\mathtt{FDecom}$ and therefore takes time at least $t_{\mathrm{fd}}$.

# Querying

In the security game IND-CCA, $\mathcal{A}$ has oracle access to $\texttt{FDecom}$ except for $\texttt{FDecom}(\mathbf{crs}, \mathbf{C}_b)$.

- $\texttt{FDecom}(\mathbf{crs}, E', K', u_b) = \texttt{FDecom}(\mathbf{crs}, E_s, K_T, u_b) = m_b$ for $E'/\langle K' \rangle$ isomorphic to $E_T \cong E_s/\langle K_T \rangle$.
- Deciding if $E'/\langle K' \rangle$ is isomorphic to $E_T$ is difficult without computing the corresponding isogeny with kernel $\langle K' \rangle$.
- Isogenies of large prime degree can not be computed efficiently.
- If $\operatorname{ord} K'$ is a large prime, the oracle can not be computed efficiently.

## Adapted IND-CCA

For the commitment $\mathbf{C}_b = (E_s, K_T, u_b)$ we need to to disallow queries of the form $\texttt{FDecom}(\mathbf{crs}, E', K', \cdot)$ if $E'/\langle K' \rangle$ is isomorphic to $E_T \cong E_s/\langle K_T \rangle$ or if $\operatorname{ord} K' \nmid d_T$.

# Binding

**Lemma (Perfect Binding)**

*A valid commitment* $\mathbf{C} = (E_s, K_T, u)$ *fixes a unique message* $m \in M$.

**Proof.**

$E_s$ and $K_T \in E_s$ fix $E_T \cong E_s/\langle K_T \rangle$ up to isomorphism and $j_T = j(E_T)$ is unique.
$F$ is a function, $u, F(j_T) \in M$ and $M$ is an additive group. Therefore $m = u \oplus F(j_T)$ is unique. □

Using the shortcut gives $j_T$ or $j_T^p$ and $F(j_T) = F(j_T^p)$.

If $\texttt{DecVrfy}(\mathbf{crs}, \mathbf{C}, m, \pi_{\text{dec}})$ and $\texttt{DecVrfy}(\mathbf{crs}, \mathbf{C}, m', \pi'_{\text{dec}})$ output **accept**, then $m \ominus F(j_T) = m' \ominus F(j_T)$ and hence $m = m'$.

If $\texttt{DecVrfy}$ accepts $(\mathbf{crs}, \mathbf{C}, m, \pi_{\text{dec}})$, then $u = m \ominus F(j_T)$ and $\texttt{FDecom}$ outputs the correct $m = u \oplus F(j_T)$.