Semi-Commutative Masking: A Framework for Isogeny-based Protocols, with an Application to Fully Secure Two-Round Isogeny-based OT

Cyprien Delpech de Saint Guilhem[1,2][0000−0002−0147−2566], Emmanuela Orsini[1][0000−0002−1917−1833], Christophe Petit[3,4][0000−0003−3482−6743], and Nigel P. Smart[1,2][0000−0003−3567−3304]

[1] imec-COSIC, KU Leuven, Belgium
[2] Dept Computer Science, University of Bristol, United Kingdom
[3] School of Computer Science, University of Birmingham, United Kingdom
[4] Département d'informatique, Université libre de Bruxelles, Belgium
cyprien.delpechdesaintguilhem@kuleuven.be, emmanuela.orsini@kuleuven.be, christophe.f.petit@gmail.com, nigel.smart@kuleuven.be

Abstract. We define semi-commutative invertible masking structures which aim to capture the methodology of exponentiation-only protocol design (such as discrete logarithm and isogeny-based cryptography). We give an instantiation based on the semi-commutative action of isogenies of supersingular elliptic curves, in the style of the SIDH key-exchange protocol. We then construct an oblivious transfer protocol using this new structure and prove that it UC-securely realises the oblivious transfer functionality in the random-oracle-hybrid model against passive adversaries with static corruptions. Moreover, we show that it satisfies the security properties required by the compiler of Döttling et al. (Eurocrypt 2020), achieving the first fully UC-secure two-round OT protocol based on supersingular isogenies.

1 Introduction

Since its beginnings, isogeny-based cryptography has progressed in several directions. First, that of protocol design, where primitives such as key-exchange and identification protocols [27, 17, 20] or signature schemes [24], have already been constructed. Secondly, in the understanding of the concrete security of the computational assumptions [23]. Finally, in the implementation methods for such protocols [15, 3, 19].

Whilst development of discrete-logarithm-based protocols has been rich, in terms of number of primitives, in the context of isogeny-based systems there has been less success. One reason is that the subtleties of isogeny-based primitives can be counter-intuitive (and even dangerous when misunderstood [22]). In particular, as noted in [27, 17], isogeny-based systems lack the commutative property which is often exploited in discrete-logarithm-based cryptography. Furthermore, the space of computational problems and their precise formulation is still shifting.

Supersingular isogeny-based protocols have attracted increasing attention mainly for their potential for post-quantum cryptography. In this direction some recent works [38, 7, 4] have proposed oblivious transfer (OT) protocols based on the hardness of supersingular isogeny problems. OT, originally introduced by Rabin in 1982 [34], is a fundamental primitive that has been proved complete for both two-party and multi-party computation, and has been used as building block in many efficient protocols [31, 28, 39]. Due to earlier interest in lattice-based and code-based cryptography, there have already been post-quantum OT protocols [32, 5, 6] based on the LWE, LPN and McEliece assumptions.

As well as underlying security assumptions, when we consider the state-of-the art in post-quantum OT protocols we also need to take into account different factors, such as the security model and round complexity. Indeed, one of the most desiderable properties, is having OT protocols with high security guarantees and only two rounds of communication. However, this is very hard to achieve and especially in the malicious setting, when one of the parties involved in the computation can arbitrarily deviate from the protocol. Indeed two-round OT with simulation based security is impossible in the plain model [26], and we need to rely on setup assumptions such as a common reference string or a random oracle.

Our contribution. We consider a new approach for studying isogeny-based constructions by defining a new general framework for exponentiation-only protocols. We then apply this new structure and describe a simple oblivious transfer protocol with high security guarantees and minimal round complexity.

Semi-commutative masking. We define new structures called *semi-commutative invertible masking schemes* to capture the exponentiation-only restriction of isogeny-based protocols and help draw out parallels with discrete-logarithm-based protocols. These also capture the absence of full commutativity in supersingular isogenies within a framework that is notationally simpler. In the full version, we show that these structures can also be realised in the discrete logarithm-based setting and in the setting of class group actions on endomorphism rings [12]. Moreover, we define generic computational problems for our structure and show that these correspond closely to the existing problems in the literature. The combination of our new structure together with instantiation-independent computational problems enables a clearer protocol design methodology. Furthermore, we believe that the hardness assumptions that we present can be extended to ones where more elements are given as a challenge (for example as used in pairing-based crypto). Such extended assumptions may enable the generic construction of schemes and protocols with richer functionalities as they have in the discrete-logarithm setting.

Isogeny-based oblivious transfer. We illustrate the advantage of our framework describing a new two-round OT protocol constructed from our masking schemes. It achieves universal composability (UC) security against passive adversaries with static corruptions in the random oracle model (ROM). In the full version we also show a second construction which is an adaptation of the key-exchange based protocol of Chou and Orlandi [14] to the "exponentiation-only" setting. Notably, our new structure allows us to provide a single proof of security for each protocol which is then valid for different instantiations of the masking scheme.

UC-secure isogeny-based two-round OT. This only provides a two-round passively secure protocol, however we also show how to obtain a two-round maliciously secure protocol. The known methods for maliciously-secure OT are either based on zero-knowledge proofs or on "lossy" encryption schemes [32], which we don't know how to instantiate using isogeny-based constructions and/or without increasing the round complexity. In [18], Döttling et al. introduced a general compiler to transform a rather weak and simple two-round *elementary*-OT (eOT), to a fully UC-secure two-round OT, providing also two instantiations: one based on the Computational Diffie-Hellman (CDH) problem and one on the Learning Parity with Noise (LPN) problem. We show (in Appendix 6) that our protocol satisfies the security requirements of this compiler, establishing the feasibility of two-round UC-secure OT based on semi-commutative masking, and more in particular on supersingular isogenies assumptions. In fact, we achieve the stronger notion of *search*-OT (sOT) security which means that Döttling et al's expensive transformation from eOT to sOT is not required for our protocol. To do so, we introduce a new problem for our masking scheme, called ParallelDouble (Definition 13), that is comparable to the one-more static CDH problem (where the adversary has access to both a challenger and a helper oracle and has to solve one more challenge than it was helped on).

Related work. Since De Feo and Jao's work [27, 17], others have explored different directions of supersingular isogenies [15, 3, 23, 24, 19, 20, 12, 35, 2, 21, 30]. However, to the best of our knowledge, our work is the first to present a framework for "exponentiation-based" protocols which unifies supersingular isogenies with previous constructions and also provides a separation between protocol design and analysis of computational assumptions. While we only present an OT protocol is this work, we believe that most of the works stated above can be formulated within our framework.

Recent works, concurrent and posterior to ours, have also proposed OT protocols based on supersingular isogenies [38, 4, 8]. The first describes an instantiation which is comparable to ours, especially regarding the computation of inverses and the question of the Weil pairing. It also proposes two protocols inspired by the same exponentiation-based approach and constructed from the same key-exchange and key-transport mechanisms. However, thanks to our new structure, our protocols better refine and separate the required computations. The OT protocol that we describe in this current paper fixes the two elements it requires for all instances, thus reducing the exchange to two flows – the best that can be hoped for, and the maximum allowed for Döttling et al.'s transformation to achieve UC security – instead of three, and it shifts the burden

Functionality $\mathcal{F}_{\mathsf{OT}}$

Parameter: n length of the bit-strings

- Upon receiving $(P_S, \mathsf{sid}, \mathsf{m}_0, \mathsf{m}_1)$ from P_S, check if a $(\mathsf{sid}, \mathsf{c})$ was previously stored. If yes, send m_c to P_R; if not, store $(\mathsf{sid}, \mathsf{m}_0, \mathsf{m}_1)$ and continue to run.
- Upon receiving $(P_R, \mathsf{sid}, \mathsf{c})$ from P_R, check if a $(\mathsf{sid}, \mathsf{m}_0, \mathsf{m}_1)$ was previously stored. If yes, send m_c to P_R; if not, store $(\mathsf{sid}, \mathsf{c})$ and continue to run.

Fig. 1: Oblivious transfer functionality

Functionality $\mathcal{F}_{\mathsf{RO}}$

The functionality is parametrized by a domain $\mathcal{D}$ and range $\mathcal{R}$. It keeps a list L of pairs of values, which is initially empty and proceeds as follows:

- Upon receiving a value $(\mathsf{sid}, m), m \in \mathcal{D}$, if there is a pair $(m, \hat{h})$, $\hat{h} \in \mathcal{R}$, in the list L, set $h = \hat{h}$. Otherwise choose $h \overset{\$}{\leftarrow} \mathcal{R}$ and store the pair (m, h) in L.
- Reply to the activating machine with (sid, h).

Fig. 2: Random oracle functionality

of computing the inverse to the Receiver. This reduces communication further and allows for only one inverse computation to be required. Using our masking structure, we also give another OT protocol, described in the full version, which separates the transmission of key material and choice material from the Sender to the Receiver. This permits the Sender to contribute to the final encryption key which is closer in spirit to the original key-exchange protocol. Vitse [38] also proposes an instantiation of her protocols from Kummer varieties; we leave it to further work to establish whether this could yield a new instantiation of our masking structure. Note, the works [4, 38] only prove security in the stand-alone and game-based models respectively, as opposed to our proofs in the UC model and there is no extension to malicious security.

Following the blueprint of previous works [10, 5], Branco et al. [8] achieve active security for OT at the cost of three additional rounds of communication. However, this requires the addition of a new mechanism which diverges from the "exponentiation-only" methodology. Furthermore, the security of their isogeny-based mechanism relies on assumptions that were only recently proposed [4] and have not yet been studied at length.

2 Preliminaries

We denote by λ the computational security parameter. We say that a function $f : \mathbb{N} \to \mathbb{N}$ is *negligible*, respectively *noticeable* (or non-negligible), if for every positive polynomial $p(\cdot)$ and all sufficiently large n it holds that $f(n) < \frac{1}{p(n)}$, respectively $f(n) \geq \frac{1}{p(n)}$. We denote by $a \overset{\$}{\leftarrow} A$ the uniform sampling of a

from a set A, and computational and statistical indistinguishability by $\overset{c}{\approx}$ and $\overset{s}{\approx}$ respectively. We let $[n]$ denote the set $\{1, \ldots, n\}$.

Symmetric encryption. By $\mathcal{E} = \{(\mathsf{KGen}_{\mathcal{E}}, \mathsf{Enc}, \mathsf{Dec}), (\mathcal{K}_{\mathcal{E}}, \mathcal{M}_{\mathcal{E}}, \mathcal{C}_{\mathcal{E}})\}$ we denote a symmetric encryption scheme, where $\mathcal{K}_{\mathcal{E}}, \mathcal{M}_{\mathcal{E}}, \mathcal{C}_{\mathcal{E}}$ are the key-space, message-space and ciphertext-space, respectively. We make use of the usual definition of $\mathsf{IND\text{-}CPA}$ security.

UC security of oblivious transfer. We prove security of our protocols in the universal composition (UC) framework of Canetti [11], and assume familiarity with this. In particular, we prove in the full version that our protocol UC-realize the OT functionality $\mathcal{F}_{\mathsf{OT}}$ in the $\mathcal{F}_{\mathsf{RO}}$-hybrid model, where $\mathcal{F}_{\mathsf{OT}}$ and $\mathcal{F}_{\mathsf{RO}}$ are presented in Figures 1 and 2.

3 Semi-Commutative Invertible Masking Structures

We first formally define our new masking structures and discuss some computational problems that arise in this setting. To help fix ideas we illustrate our masking structures with the case of discrete logarithms in a finite field $\mathbb{F}_p$, where $q = (p-1)/2$ is prime and $g \in \mathbb{F}_p$ is an element of order q.

3.1 Masking Structure

A masking structure $\mathcal{M}$ is defined over a set X. Each element $x \in X$ may have multiple *representations*, and we define R_x to be the set of representations of an element $x \in X$. (We require that it be efficient to recover x from any representation in R_x.) We denote the set of all such sets by $R_X = \{R_x\}_{x \in X}$. The sets of representatives are assumed to be disjoint, i.e. $\forall x, x' \in X$ s.t. $x \neq x'$, $R_x \cap R_{x'} = \emptyset$, and we define $R = \cup_{x \in X} R_x$ to be the set of all representatives. For example, if we take $X = \langle g \rangle \subset \mathbb{F}_p^*$, then the usual choice for R is to let $R_x = \{x\}$ for every $x \in X$; but one could also take a redundant representation with two elements letting $R_x = \{x, x+p\}$.

A *mask* is a function $\mu : R \longrightarrow R$, and a masking set M is a set of such functions. In the discrete logarithm case, a natural candidate for M is a set indexed by elements in $\mathbb{Z}_q^*$ which each give an explicit exponentiation algorithm on the set of representatives of the group elements X. A masking function $\mu \in M$ is said to be *invertible* if

$$\forall x \in X, \quad \forall r \in R_x, \quad \exists \mu^{-1} \in M \quad : \quad \mu^{-1}(\mu(r)) \in R_x. \tag{1}$$

Note, we only require that μ^{-1} outputs a representative in the same set R_x. If all elements $\mu \in M$ are invertible, then we say that the masking set M is *invertible*. In the discrete logarithm case, if μ corresponds to the map $g \mapsto g^a$, then μ^{-1} corresponds to the map $g \mapsto g^{1/a}$.

An *invertible masking structure* $\mathcal{M}$ for a set X is then a collection of sets of representative R_X, along with a collection of invertible masking sets $[M_i]_{i=1}^n$,

```
Data: $\mathcal{M} = \{X, R_X, [M_i]_{i=1}^n\}$, $\lambda \in \mathbb{N}$
Result: $\mathsf{win} \in \{0,1\}$
$r, \mu_0, \mu_1, i, \mathsf{st} \leftarrow \mathcal{A}(1^\lambda)$ such that $r \in R$, $i \in [n]$, $\mu_0, \mu_1 \in M_j$, $j \neq i$;
$r_0 \leftarrow \mu_0(r), \quad r_1 \leftarrow \mu_1(r)$;
$\mathsf{b} \xleftarrow{\$} \{0,1\}$;
$\mu \xleftarrow{\$} M_i$;
$\tilde{r} \leftarrow \mu(r_\mathsf{b})$;
$\tilde{\mathsf{b}} \leftarrow \mathcal{A}(1^\lambda, \mathsf{st}, \tilde{r})$;
if $\tilde{\mathsf{b}} = \mathsf{b}$, then return $\mathsf{win} = 1$ else return $\mathsf{win} \xleftarrow{\$} \{0,1\}$;
```

Fig. 3: The $\mathsf{IND\text{-}Mask}_{\mathcal{A},\mathcal{M}}$ security experiment

and we write $\mathcal{M} = \{X, R_X, [M_i]_{i=1}^n\}$. Such an invertible masking structure is said to be *semi-commutative* if

$$\forall i \neq j,\ \ \forall \mu \in M_i,\ \ \forall \mu' \in M_j,\ \ \forall r \in R,\ \ \mu(\mu'(r)) \in R_x \iff \mu'(\mu(r)) \in R_x. \quad (2)$$

In the discrete logarithm case, with M a set of exponentiation functions, $\mathcal{M} = \{X, R_X, [M, M]\}$ is straightforwardly semi-commutative.

3.2 Problems and Properties

We now present a distinguishing experiment and computational problems for masking structures. The precise security level of these depends from concrete instantiations and reductions to specific computational problems.

Definition 1 (IND-Mask security). *We define the $\mathsf{IND\text{-}Mask}_{\mathcal{A},\mathcal{M}}$ experiment in Figure 3 for a masking structure $\mathcal{M} = \{X, R_X, [M_i]_{i=1}^n\}$, and an arbitrary adversary $\mathcal{A}$. We say that $\mathcal{M}$ is* IND-Mask-secure *if for all PPT adversaries $\mathcal{A}$, it holds that*

$$\left| \Pr\left[\mathsf{IND\text{-}Mask}_{\mathcal{A},\mathcal{M}}(\lambda) = 1\right] - \frac{1}{2} \right| \leq \mathsf{negl}(\lambda).$$

In the discrete logarithm setting, when $R_x = \{x\}$, the map $g \mapsto g^a$ for random $a \in \mathbb{Z}_q^*$ induces a random permutation of the group elements. Therefore for a secret a and two group elements g_0, g_1, the distribution of g_b^a is perfectly uniform, independently of b. This shows that such an $\mathcal{M}$ is perfectly IND-Mask-secure.

Note 1. In some settings (but not in the discrete logarithm one), it may be possible to distinguish the action of two masks that belong to separate masking sets. It is also possible that this difference is preserved under the action of a mask from a third masking set. Therefore, if an adversary was able to submit arbitrary r_0 and r_1 to the IND-Mask experiment, it could ensure that the difference between them is preserved by the action of the randomly sampled μ and hence win the experiment with certainty. By forcing $\mathcal{A}$ to submit a single $r \in R$ and two maps μ_0, μ_1 belonging to the same masking set M_j, the experiment prevents that strategy.

We also define to the following hard problems for semi-commutative invertible masking structures:

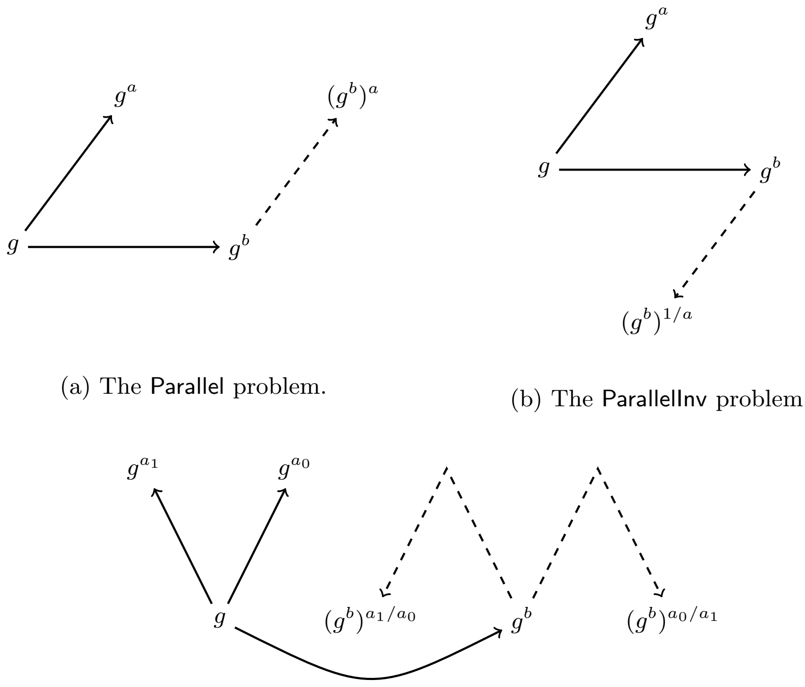
Definition 2. *Given a masking structure $\mathcal{M} = \{X, R_X, [M_i]_{i=1}^n\}$, we define the following computational problems:*

1. Demask*: Given (i, r, r_x) with the promise that $r_x = \mu_x(r)$ for a uniformly random $\mu_x \xleftarrow{\$} M_i$, return μ_x.*
2. $\mathsf{Parallel}$*: Given (i, j, r, r_x, r_y) with the promise that $i \neq j$ and that $r_x = \mu_x(r)$ and $r_y = \mu_y(r)$ for uniformly random $\mu_x \xleftarrow{\$} M_i, \mu_y \xleftarrow{\$} M_j$, return $z \in X$ such that $\mu_x(r_y) \in R_z$.*
3. $\mathsf{ParallelInv}$*: Given (i, j, r, r_x, r_y) with the promise that $i \neq j$ and that $r_x = \mu_x(r)$ and $r_y = \mu_y(r)$ for uniformly random $\mu_x \xleftarrow{\$} M_i, \mu_y \xleftarrow{\$} M_j$, return $z \in X$ such that $\mu_x^{-1}(r_y) \in R_z$.*
4. $\mathsf{ParallelEither}$*: Given (i, j, r, r_x, r_y) with the promise that $i \neq j$ and that $r_x = \mu_x(r)$ and $r_y = \mu_y(r)$ for uniformly random $\mu_x \xleftarrow{\$} M_i, \mu_y \xleftarrow{\$} M_j$, return $z \in X$ such that either $\mu_x(r_y) \in R_z$ or $\mu_x^{-1}(r_y) \in R_z$.*
5. $\mathsf{ParallelBoth}$*: Given $(i, j, r, r_{x_0}, r_{x_1}, r_y)$ with the promise that $i \neq j$ and that $r_{x_\mathsf{b}} = \mu_\mathsf{b}(r), \mathsf{b} \in \{0,1\}$ and $r_y = \mu_y(r)$ for uniformly random $\mu_\mathsf{b} \xleftarrow{\$} M_i, \mu_y \xleftarrow{\$} M_j$, return $z \in X$ such that either $\mu_{1-\mathsf{b}}^{-1}(\mu_\mathsf{b}(r_y)) \in R_z$ or $\mu_\mathsf{b}^{-1}(\mu_{1-\mathsf{b}}(r_y)) \in R_z$.*

To make explicit the given structure $\mathcal{M}$ to which the (say) Demask *problem refers, we write $\mathsf{Demask}^{\mathcal{M}}$. The name "*$\mathsf{Parallel}$*" is inspired by a similar problem defined by Couveignes [16].*

We motivate these problems in the context of the discrete logarithm setting, where we take our masking structure as before to have $R_x = \{x\}$ and to have each M_i to be identical to the set of exponentiation maps indexed by $\mathbb{Z}_q^*$. We give a graphical intuition of these problems in Figure 4.

- The Demask problem is, given (g, h) with the promise that $h = g^a$ for a random a, to return a. This is the discrete logarithm problem (DLP).
- Similarly, the $\mathsf{Parallel}$ problem is, given (g, g^a, g^b) for random a, b, to return $g^{a \cdot b}$ which is the computational Diffie-Hellman (CDH) problem.
- In the discrete logarithm setting, the $\mathsf{ParallelInv}$ problem is to compute $g^{b/a}$ given (g, g^a, g^b). In the full version we show that this is equivalent to the $\mathsf{Parallel}$ problem. We note that this does not immediately hold in the abstract case, due to the absence of relation between r and $\mu^{-1}(\mu(r))$, but it can nonetheless be shown to hold for different instantiations.
- The $\mathsf{ParallelEither}$ problem is an instance where both the solutions to the $\mathsf{Parallel}$ and to the $\mathsf{ParallelInv}$ problems, for the same challenge, are accepted. Whilst it is immediate that the $\mathsf{ParallelEither}$ problem is at most as hard as any of the other two, a formal reduction to show the reverse implication does not appear to be as trivial. We conjecture that in most settings, and in the discrete logarithm setting in particular, allowing for two possible answers which are both hard to compute on their own does not significantly decrease the hardness of the $\mathsf{ParallelEither}$ problem.



(a) The Parallel problem.

(b) The ParallelInv problem.

(c) The ParallelBoth problem.

Fig. 4: Representations of computational problems.

- The solution of the ParallelBoth problem can be seen as a combination of both Parallel and ParallelInv solutions together with the choice of the ParallelEither problem as is shown in Figure 4c.
  Indeed, one can first use a Parallel oracle to compute $\mu_{\mathsf{b}}(r_y)$ for either $\mathsf{b} \in \{0, 1\}$ and then use a ParallelInv oracle to compute $\mu^{-1}_{1-\mathsf{b}}(\mu_{\mathsf{b}}(r_y))$ which shows that ParallelBoth is at most as hard as those two problems. Similarly to the ParallelEither problem, we conjecture that in most settings the ParallelBoth will not be significantly easier as it requires solutions which are both hard to compute.

4 Instantiation From Supersingular Isogenies

To avoid a sub-exponential quantum attack vector [13], De Feo, Jao and Plût [17] consider the use of supersingular elliptic curves over the extension field $\mathbb{F}_{p^2}$ whose *full* endomorphism ring is an order in a quaternion algebra and therefore non-commutative. In this section we summarize this approach succinctly, construct a semi-commutative masking structure from this setting and discuss the hardness of the induced problems.

4.1 Supersingular Isogenies over the Extension Field

Preliminaries. Let E_1 and E_2 be elliptic curves defined over a finite field $\mathbb{F}_q$. An *isogeny* $\phi : E_1 \to E_2$ over $\mathbb{F}_q$ is a non-constant rational map over $\mathbb{F}_q$ which is also a group homomorphism from $E_1(\mathbb{F}_q)$ to $E_2(\mathbb{F}_q)$. For the isogenies that we consider, we identify their degrees with the size of their kernels. Two curves E_1, E_2 are said to be *isogenous* over $\mathbb{F}_q$ if there exists an isogeny $\phi : E_1 \to E_2$ over $\mathbb{F}_q$; this holds if and only if $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$. A set of elliptic curves over $\mathbb{F}_q$ that are all isogenous to one another is called an *isogeny class.*

An *endomorphism* over $\mathbb{F}_q$ of an elliptic curve E is a particular isogeny $E \to E$ over $\mathbb{F}_{q^m}$ for some m. The set of endomorphisms of E together with the zero map, denoted $\mathrm{End}(E)$, forms a ring under the addition, $\phi \oplus \varphi : P \mapsto \phi(P) + \varphi(P)$, and multiplication, $\phi \otimes \varphi : P \mapsto \phi(\varphi(P))$, operations. The full ring $\mathrm{End}(E)$ is isomorphic to either an order in a quaternion algebra, in which case we say that E is supersingular, or to an order in an imaginary quadratic field, in which case we say that E is ordinary. Curves that are in the same isogeny class are either all supersingular or all ordinary. Here we focus on the supersingular case. All supersingular curves can be defined over the field $\mathbb{F}_{p^2}$ for a prime p and for every prime $\ell \nmid p$ there exist $\ell + 1$ isogenies, up to isomorphism, of degree ℓ originating from any given supersingular curve.

Given a curve E and a subgroup K of E there is, up to isomorphism, a unique isogeny $\phi : E \to E'$ having kernel K and we therefore identify E' with the notation E/ϕ. Particularly, we will work with subgroups of the torsion group $E[m]$ for $m \in \mathbb{N}$ which is the group of points of E whose order divides m. When we also have that m^2 divides $\#E(\mathbb{F}_{p^2})$, we can always represent cyclic kernels by generators defined over $\mathbb{F}_{p^2}$.

Semi-commutativity. We introduce the notion of *semi-commutativity* present in this setting; the same notion is behind the SIDH key-exchange protocol [17] and we generalise it here. We discuss the case where $\mathbb{F}_q$ is fixed to be $\mathbb{F}_{p^2}$ where p is a prime of the form $\ell_1^{e_1} \ell_2^{e_2} \cdots \ell_n^{e_n} \cdot f \pm 1$ for n small primes $\ell_1, \ldots, \ell_n$ and a small cofactor f. By construction, in each isomorphism class there is a curve $E/\mathbb{F}_{p^2}$ such that the torsion group $E[\ell_i^{e_i}]$ contains $\ell_i^{e_i-1}(\ell_i + 1)$ cyclic subgroups of order $\ell_i^{e_i}$ (which each define a different isogeny).

To compute and publish a curve resulting from a secret isogeny, a party generates a secret key by selecting a random point K_i of order $\ell_i^{e_i}$ on a curve E and computes a public curve by computing the unique isogeny with kernel $\langle K_i \rangle$ and publishing the domain curve $E/\langle K_i \rangle$. The issue here is that the structure of $\mathrm{End}(E)$ no longer allows for arbitrary isogenies to commute and an analogue of the $(g^a)^b = (g^b)^a$ equality is not immediate. However, with isogenies of co-prime degrees some commutative structure remains.

To solve this, in addition to the curve E, the parties agree on bases $\{P_i, Q_i\}$ for each of the torsion groups $E[\ell_i^{e_i}]$. The semi-commutative structure then emerges since applying an isogeny of degree $\ell_i^{e_i}$ preserves the torsion groups $E[\ell_j^{e_j}]$ for $j \neq i$. Therefore, alongside publishing $E/\langle K_i \rangle$ for their secret isogeny ϕ_i, parties also publish $\{\{\phi_i(P_j), \phi_i(Q_j)\}_{j \neq i}\}$, the images under ϕ_i of the bases for the other torsion groups. By expressing their secret kernel as $K_j = [\alpha_j]P_j + [\beta_j]Q_j$ and applying α_j, β_j to $\{\phi_i(P_j), \phi_i(Q_j)\}$, the other party can then compute an isogeny $\varphi_j : E/\langle K_i \rangle \to E/\langle K_i, K_j \rangle$ which is "parallel" to the isogeny $\phi_j : E \to E/\langle K_j \rangle$ in the sense of Figure 4a.

Whilst the two resulting curves $E/\langle K_i, K_j \rangle$ and $E/\langle K_j, K_i \rangle$ may not be identical, they will be isomorphic, and the parties can then take the j-invariants of their respective curves as an identical shared value.

The Weil pairing. We recall here the notion of the *Weil pairing*. For any integer $m \in \mathbb{N}$, we let $\zeta_m = \{u \mid u^m = 1\} \subset \mathbb{F}_{p^2}^*$. For any curve $E/\mathbb{F}_{p^2}$, the Weil pairing is a map $e_m : E[m] \times E[m] \longrightarrow \zeta_m$, that satisfies $e_m(\phi(P), \phi(Q)) = e_m(P, Q)^{\deg(\phi)}$, where $\phi : E \to E'$ is any isogeny.

4.2 Masking Structure

To define a semi-commutative masking structure, we fix $p = \ell_1^{e_1} \ell_2^{e_2} \cdots \ell_n^{e_n} \cdot f \pm 1$ as above. In this setting, there are five supersingular isogeny classes and we let X denote one of the two classes with curves $E/\mathbb{F}_{p^2}$ with trace $t = p^2 + 1 - \#E(\mathbb{F}_{p^2}) \in \{-2p, 2p\}$; these two classes are the largest of the five [1].

Representatives. For each j-invariant $x \in X$, there is a canonical choice of curve E_x [36]. For each E_x we take the appropriate twist of the curve such that they belong to the same isogeny class. We define the set R_x of representatives as the set of tuples $(E_x, \{\{P_i, Q_i\}_{i \in [n]}\})$ where $\{P_i, Q_i\}$ is a basis of the torsion group $E_x[\ell_i^{e_i}]$ as above.

For a given curve and torsion order, there exists a deterministic and efficient algorithm $\mathsf{Basis}(E, i)$ which outputs a basis $\{P_i, Q_i\} \subset E_x[\ell_i^{e_i}]$ [3, Section 3.2]; for each torsion order, we fix a generator $q_i \in \zeta_{\ell_i^{e_i}}$ such that for any curve E, $e_m(P_i, Q_i) = q_i$ for $\{P_i, Q_i\} \leftarrow \mathsf{Basis}(E, i)$. This will be used to derive new torsion points when required, but these are still free to be modified under the action of isogenies. Hence for each x, there will be a unique choice of E_x but many choices of bases of torsion groups that originate from the deterministic one.

Masking sets. We first observe that for any $K_i = [\alpha_i]P_i + [\beta_i]Q_i$ on E, the point $[m]K_i$, for $m \in (\mathbb{Z}/\ell_i^{e_i}\mathbb{Z})^*$, generates the same subgroup of $E[\ell_i^{e_i}]$. By defining the equivalence relation $\sim_R$ by

$$(\alpha, \beta) \sim_R (\alpha', \beta') \qquad \iff \qquad \exists m \in (\mathbb{Z}/\ell_i^{e_i}\mathbb{Z})^* \text{ s.t. } (\alpha', \beta') = (m\alpha, m\beta),$$

we can then identify any such K_i with the equivalence class of (α_i, β_i) which we denote $[\alpha_i : \beta_i]$. We recall that the projective line $\mathbb{P}^1(\mathbb{Z}/\ell_i^{e_i}\mathbb{Z})$ is the set of equivalence classes $[\alpha_i : \beta_i]$ such that $\gcd(\alpha_i, \beta_i) = 1$.

Since K_i has exact order $\ell_i^{e_i}$, at least one of α_i and β_i must not be divisible by ℓ_i and hence the ideal of the ring $\mathbb{Z}/\ell_i^{e_i}\mathbb{Z}$ generated by α_i, β_i is always the unit ideal, i.e. the whole of $\mathbb{Z}/\ell_i^{e_i}\mathbb{Z}$. This implies that all the possible choices for K_i can be exactly identified with the points on the projective line $\mathbb{P}^1(\mathbb{Z}/\ell_i^{e_i}\mathbb{Z})$. We therefore define n masking sets $[M_i]_{i\in[n]}$ where each M_i is the projective line $\mathbb{P}_i := \mathbb{P}^1(\mathbb{Z}/\ell_i^{e_i}\mathbb{Z})$.

Masking action. Computing the result of a mask $\mu(r) \in R_y$ on a representative $r \in R_x$ then consists in computing one of its representatives K_i in $E_x[\ell_i^{e_i}]$ and the isogeny $\phi_i : E_x \to E_x/\langle K_i\rangle$. Note that the curve $E_x/\langle K_i\rangle$ with j-invariant $y \in X$ may not be the same curve as the canonical choice E_y. However they will be isomorphic over $\mathbb{F}_{p^2}$, due to the appropriate choice of twist in the definition of our set R_y, and the isomorphism $\chi : E_x/\langle K_i\rangle \longrightarrow E_y$ will be easy to compute.

To be able to compose isogenies in a semi-commutative way, computing $\mu(r)$ also requires computing the images of $\{\{P_j, Q_j\}\}$ for $j \neq i$ first under ϕ_i and then under the isomorphism χ to obtain bases of the torsion groups of E_y. It also requires generating a new basis for $E_y[\ell_i^{e_i}]$ using the $\mathsf{Basis}(E_y, i)$ algorithm.

The output of the computation of the mask $\mu(r)$ is therefore the curve $E_y \overset{\chi}{\simeq} E_x/\langle K_i\rangle$ together with the basis points $\{\{\chi\circ\phi_i(P_j), \chi\circ\phi_i(Q_j)\}\}$ for $j \neq i$ and the output of $\mathsf{Basis}(E_y, i)$.

Inverting the mask. Since our masking sets M_i do not derive from a group structure, we do not have an immediate instantiation of an inverse operation. However, for every isogeny $\phi : E \to E'$ of degree ℓ, there is a unique dual isogeny $\hat{\phi} : E' \to E$ also of degree ℓ such that the composition is the multiplication-by-ℓ map: $\hat{\phi}\circ\phi = [\ell] : E \to E$. Whilst not a perfect inverse operation, in this setting the multiplication-by-$\ell_i^{e_i}$ map preserves the structure of the $\ell_j^{e_j}$-torsion groups for all $j \neq i$ and that is all we require for semi-commutativity to hold.

Hence, given a kernel generator $K_i \in E[\ell_i^{e_i}]$ for some curve E, one can compute a generator of the image $\phi_i(E[\ell_i^{e_i}]) \subset E'[\ell_i^{e_i}]$ of the $\ell_i^{e_i}$-torsion group under the isogeny $\tilde{\phi}_i$ defined by K_i and an appropriate isomorphism, to obtain $\hat{K}_i \in E/\langle K_i\rangle$ which is a generator of the kernel of the unique dual isogeny $\hat{\phi}_i$.

Given a mask $\mu \in M_i = \mathbb{P}_i$ and elements r and $r' = \mu(r)$ with $r' = (E', \{\{P_j, Q_j\}_{j\in[n]}\})$, computing the inverse μ^{-1} amounts to computing a point $\hat{K}_i$ as above and expressing it as $(\hat{\alpha}_i, \hat{\beta}_i)$ in the deterministically generated basis for $E'[\ell_i^{e_i}]$ which can be done efficiently as is shown in [3]. This then allows us to define μ^{-1} uniquely as $[\hat{\alpha}_i : \hat{\beta}_i] \in \mathbb{P}_i$, given μ and r. We note that the dependency of μ^{-1} on μ and r is consistent with the definition of the inverse of a mask as stated in Section 3.

Masking structure. We formally define a masking structure in this setting.

Definition 3 (Masking structure from supersingular isogenies). *Let p be a prime defining the finite field $\mathbb{F}_{p^2}$ as above, we define the masking structure $\mathcal{M}_p = \{X, R_X, [M_i]_{i\in[n]}\}$ where the individual components are defined as above.*

Lemma 1. *The masking structure $\mathcal{M}_p$ of Definition 3 is semi-commutative.*

Proof. First we see that the elements of $\mathcal{M}_p$ together with the action of any $\mu \in M_i$ on any r are well-defined. Then, since the composition of any isogeny with its dual results in an endomorphism of the starting curve, our method of inverting a given mask yields the same j-invariant regardless of the starting r or masking index i. Also, the semi-commutative property of our structure follows from the semi-commutative property of isogenies of co-prime degrees. Finally, the required efficiency of the computations for $\mathcal{M}_p$ follows from the comments above regarding the computation of isogenies of smooth degrees and expression of points in arbitrary torsion bases. Equality in X and M_i and membership in X are immediate to check. □

4.3 Computational Problems

The problem landscape of the SIDH setting is still currently undergoing intense study from the community. Urbanik and Jao [37] have proposed a detailed presentation and study of the analogues of the discrete logarithm and CDH problems that arise from the SIDH key-exchange of De Feo, Jao and Plût [17]. Galbraith and Vercauteren also have written a survey of these problems [25], with a stronger focus on the mathematics of isogenies of elliptic curves.

Here we frame Urbanik and Jao's discussion of these problems in [37, Section 4] in our setting that uses n distinct small primes ℓ_i. Whilst we give a very general presentation, in practice the OT scheme presented in this paper will only require $n = 2$, as in the case of the SIDH key-exchange. Our second OT protocol (described in the full version) will require $n = 3$, which constitutes only a small extension of the original setting.

The isogeny problem. In its simplest form, the intuition behind the security of isogeny-based cryptography is that it is hard to compute a hidden isogeny, up to isomorphism, when given only the initial and final j-invariants. The *general isogeny problem* can be stated as follows.

Definition 4 (General isogeny problem [25, Definition 1]). *Given j-invariants $j, j' \in \mathbb{F}_{p^2}$, return an isogeny $\phi : E \longrightarrow E'$ (if it exists), where $j(E) = j$ and $j(E') = j'$.*

Given that the elements of X in the masking structure $\mathcal{M}_p$ are the supersingular j-invariants of $\mathbb{F}_{p^2}$ and that the elements of the masking sets M_i can be uniquely identified with isogenies between isomorphism classes, it would first seem that the Demask problem for $\mathcal{M}_p$ can be instantiated as the general isogeny problem of Definition 4. To recover some commutative structure, however, we have to reveal the images of the bases of the torsion points. This constitutes significantly more information and therefore is conjectured to be an easier problem to solve [24, 33, 25, 29].

Additional information. This has led to the definition in the literature of a specific SIDH problem. Here we merge the definitions of [25] and [37] for the case of $n = 2$ small primes in the composition of p.

Definition 5 (2-i-isogeny problem [25, Def. 2][37, Prob. 4.1]). *Let $i \in \{1, 2\}$ and let (E, P_1, Q_1, P_2, Q_2) be such that $E/\mathbb{F}_{p^2}$ is a supersingular curve and P_j, Q_j is a basis for $E[\ell_j^{e_j}]$ for $j \in \{1, 2\}$. Let E' be such that there is an isogeny $\phi : E \longrightarrow E'$ of degree $\ell_i^{e_i}$. Let P'_j, Q'_j be the images under ϕ of P_j, Q_j for $j \neq i$. The* 2-i-isogeny problem*, is, given $(E, P_1, Q_1, P_2, Q_2, E', P'_j, Q'_j)$, to determine an isogeny $\tilde{\phi} : E \longrightarrow E'$ of degree $\ell_i^{e_i}$ such that $P'_j = \tilde{\phi}(P_j)$ and $Q'_j = \tilde{\phi}(Q_j)$.*

This definition leads to the following natural generalisation which we show corresponds exactly to the computational problem that we need.

Definition 6 (n-i-isogeny problem). *Let n be an integer, $i \in \{1, \ldots, n\}$ and let $(E, \{P_j, Q_j\}_{j=1}^n)$ be a tuple such that $E/\mathbb{F}_{p^2}$ is a supersingular curve and P_j, Q_j is a basis for $E[\ell_j^{e_j}]$ for $j \in [n]$. Let E' be such that there is an isogeny $\phi : E \longrightarrow E'$ of degree $\ell_i^{e_i}$. Let $\{P'_j, Q'_j\}$ be the images under ϕ of $\{P_j, Q_j\}$ for $j \neq i$. The* n-i-isogeny problem*, for $i \in [n]$, is, given $(E, \{P_j, Q_j\}_{j=1}^n, E', \{P'_j, Q'_j\}_{j \neq i})$, to determine an isogeny $\tilde{\phi} : E \longrightarrow E'$ of degree $\ell_i^{e_i}$ such that $P'_j = \tilde{\phi}(P_j)$ and $Q'_j = \tilde{\phi}(Q_j)$ for all $j \neq i$.*

Lemma 2. *Let $p = \ell_1^{e_1} \ell_2^{e_2} \cdots \ell_n^{e_n} \cdot f \pm 1$ be a prime and let $\mathcal{M}_p$ be a masking structure as defined in Definition 3. Then the* Demask *problem for $\mathcal{M}_p$ is an instance of the n-i-isogeny problem.*

Proof. The specification of i in (i, r, r_x) together with the random mask μ_x satisfies the promise of existence of an isogeny ϕ of degree $\ell_i^{e_i}$. Also, By definition of R_x for each $x \in X$ for $\mathcal{M}_p$, the representative r_x contains exactly the information of the curve E' together with the images of the appropriate torsion points. We note that r_x does not contain additional information as the basis points of $E'[\ell_i^{e_i}]$ are derived deterministically from E'. □

Computational SIDH. The isogeny problems defined above can be viewed as the analogues of the discrete logarithm problem of computing an unknown exponent in the general case and in the specific SIDH setting. This naturally leads to an analogue of the CDH problem which is defined as follows in the case of $n = 2$.

Definition 7 (2-computational SIDH problem [37, Problem 4.3]). *Let E, E_A, E_B be supersingular curves such that there exist isogenies $\phi_A : E \longrightarrow E_A$ and $\phi_B : E \longrightarrow E_B$ with kernels K_A and K_B and degrees $\ell_1^{e_1}$ and $\ell_2^{e_2}$ respectively. Let P_1, Q_1 and P_2, Q_2 be bases of $E[\ell_1^{e_1}]$ and $E[\ell_2^{e_2}]$ respectively, and let $P'_1 = \phi_B(P_1)$, $Q'_1 = \phi_B(Q_1)$ and $P'_2 = \phi_A(P_2)$, $Q'_2 = \phi_A(Q_2)$ be the images of the bases under the isogeny of coprime degree. The* 2-computational SIDH problem *is, given $(E, P_1, Q_1, P_2, Q_2, E_A, P'_2, Q'_2, E_B, P'_1, Q'_1)$, to identify the isomorphism class of the curve $E/\langle K_A, K_B \rangle$.*

This problem can also be generalised in a natural way to the following which then yields the appropriate instantiation for our structure.

Definition 8 **(n-i,j-computational SIDH problem).** *Let E, E_A, E_B be supersingular curves such that there exist isogenies $\phi_A : E \longrightarrow E_A$ and $\phi_B : E \longrightarrow E_B$ with kernels K_A and K_B and degrees $\ell_i^{e_i}$ and $\ell_j^{e_j}$ respectively with $i \neq j$. Let $\{P_k, Q_k\}$ be bases of $E[\ell_k^{e_k}]$, for $k \in [n]$, and let $P_k^A = \phi_A(P_k)$, $Q_k^A = \phi_A(Q_k)$, for $k \neq i$, and $P_k^B = \phi_B(P_k)$, $Q_k^B = \phi_B(Q_k)$, for $k \neq j$ be the images of the bases under the isogeny of coprime degree. The* n-i,j-computational SIDH problem, *for $i, j \in [n]$, is, given $(E, \{P_k, Q_k\}_{k\in[n]}, E_A, \{P_k^A, Q_k^A\}_{k\neq i}, E_B, \{P_k^B, Q_k^B\}_{k\neq j})$, to identify the isomorphism class of the curve $E/\langle K_A, K_B\rangle$.*

Lemma 3. *Let $p = \ell_1^{e_1}\ell_2^{e_2}\cdots\ell_n^{e_n}\cdot f \pm 1$ be a prime and let $\mathcal{M}_p$ be a masking structure as defined in Definition 3. Then the* Parallel *problem for $\mathcal{M}_p$ is an instance of the n-i,j-CSIDH problem.*

Proof. As for Lemma 2, the specification (i, j, r, r_x, r_y) of the Parallel problem for $\mathcal{M}_p$ satisfies the promise of existence of the two isogenies of coprime degrees and contains all the required information on the images of the torsion bases. Also, the goals of the problems agree since the solution to the Parallel problem for $\mathcal{M}_p$ requires $z \in X$ which is exactly the j-invariant which identifies the isomorphism class uniquely. Again, r_x and r_y do not contain additional information since the bases for the ith and jth torsion groups are computed deterministically. □

Regarding the ParallelInv problem for $\mathcal{M}_p$, we do not have an immediate reduction to the Parallel problem. We discuss this in comparison to the instantiation from hard homogeneous spaces and also an interesting subtlety in the definitions of the CDH problem in the full version of this work. We nonetheless conjecture that, as they are very similar, the hardness of the ParallelInv problem is close to that of the Parallel problem. We similarly conjecture that the hardness of the ParallelEither and ParallelBoth problems is comparable to that of the Parallel and ParallelInv problems as no additional information is revealed and only similarly hard-to-compute solutions are required.

Decisional SIDH. Galbraith and Vercauteren also formalise a decisional variant of the SIDH problem in the case of $n = 2$.

Definition 9 **(2-i-decisional SIDH problem [25, Definition 3]).** *Let (E, P_1, Q_1, P_2, Q_2) be such that $E/\mathbb{F}_{p^2}$ is a supersingular curve and P_j, Q_j is a basis for $E[\ell_j^{e_j}]$ for $j \in \{1, 2\}$. Let E' be an elliptic curve and let $P_j', Q_j' \in E'[\ell_j^{e_j}]$ for $j \neq i$. Let $0 < d < e_i$. The* 2-i-decisional SIDH problem *is, given $(E, P_1, Q_1, P_2, Q_2, E', P_j', Q_j', d)$ for $j \neq i$, to determine if there exists an isogeny $\phi : E \to E'$ of degree ℓ_i^d such that $\phi(P_j) = P_j'$ and $\phi(Q_j) = Q_j'$.*

As for the computational problems, we can generalise the above problem to our setting.

Definition 10 **(n-i-decisional SIDH problem).** *Let $(E, \{P_j, Q_j\}_{j\in[n]})$ be such that $E/\mathbb{F}_{p^2}$ is a supersingular curve and P_j, Q_j is a basis for $E[\ell_j^{e_j}]$ for $j \in [n]$. Let E' be an elliptic curve and let $P'_j, Q'_j \in E'[\ell_j^{e_j}]$ for $j \neq i$. Let $0 < d < e_i$. The* n-i-decisional SIDH problem *is, given $(E, \{P_j, Q_j\}_{j\in[n]}, E', \{P'_j, Q'_j\}_{j\neq i}, d)$, to determine if there exists an isogeny $\phi : E \to E'$ of degree ℓ_i^d such that $\phi(P_j) = P'_j$ and $\phi(Q_j) = Q'_j$ for $j \neq i$.*

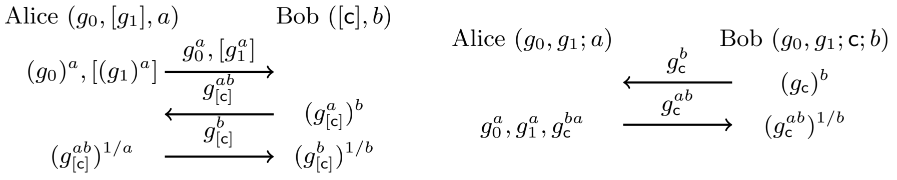
Whilst we do not have an equivalence between the IND-Mask experiment and the n-i-DSIDH as presented above, we see that an oracle for the latter with $d = e_i$ is sufficient to obtain a noticeable advantage against the former. Also, it would seem that our IND-Mask experiment corresponds to a worst case of the n-i-DSIDH as it uses a maximal degree of $d = e_i$. Given the state of the art in cryptanalysis for these problems, we conjecture that the IND-Mask problem for $\mathcal{M}_p$ is not significantly easier than the n-i-DISDH for the same parameters.

As hinted at in Note 1, the Weil pairing is in fact a useful tool against the IND-Mask experiment. Indeed, if the adversary had free control over the values r_0 and r_1 of the experiment, it could give two representatives whose basis points of the same torsion group evaluated to different values under the Weil pairing. This difference would be preserved under the secret masking action of the experiment and this would enable it to win trivially. Restricting the adversary's input to be a single representative r and two masks that determine r_0 and r_1 and preserve the values of Weil pairing on the points of r thus prevents this strategy.

Security analysis. As mentioned above, one of the main advantage of the SIDH approach as opposed to the hard homogeneous space approach (including CSIDH) is that no sub-exponential attack is known on the SIDH protocol, even using a quantum computer. On the other hand in the SIDH protocol, the action of the secret isogeny on a large torsion subgroup is revealed. A paper by Petit [33] and a recent follow-up work by Kutas et al. [29] show how to exploit this additional information to break variants of the SIDH protocol with unbalanced parameters or weak starting curves.

More precisely, let $N_1 \approx p^\alpha$ be the degree of the isogeny to compute, and let $N_2 \approx p^\beta$ be the order of torsion points images revealed in the protocol. The original SIDH protocol uses $\alpha \approx \beta \approx \frac{1}{2}$, but [33] and [29] describe a generalization to any coprime, power-smooth values N_1, N_2. Under some parameter restrictions and heuristic assumptions, the best attack in [29] computes the isogeny in classical polynomial time assuming $\beta > 2\alpha > 2$ or $\beta > 3\alpha > 3/2$. Furthermore, Kutas et al. show an attack requiring only $\beta > 2\alpha$ (with no lower bound on α) when the protocol uses a weak starting curve.

In our instantiation above, for any i one can fix $\alpha = e_i \log \ell_i$ and $\beta = \sum_{j\neq i} e_j \log \ell_j$. We also have $\alpha + \beta \leq 1$ so the first attack in [33] and its improvement in [29] does not apply if the starting curve is not weak. The second attack of [33], however, applies whenever the number n of factors ℓ_i is larger than $O(e_i \log \ell_i)$ for some i. The second one from [29] applies if any starting curve is weak. The notion of weak however depends on p, α, β and the chosen curve so



(a) The Shamir three-pass protocol and its OT variant

(b) Sketch of final OT protocol flows

Fig. 5: Sketch of the Shamir three-pass OT protocol and the final variant

choosing correct parameters (as those chosen in SIDH are) prevents this from happening.

One may fear that these attacks will get improved over time, leading to further restrictions on n. We note that $n = 3$ is sufficient to instantiate our OT protocols. Moreover, the protocol we describe in this paper could be even instantiated with $n = 2$. We note also that $n = 2$ in our construction corresponds to the SIDH protocol parameters, so our semi-commutative masking construction with $n = 2$ will remain secure as long as SIDH remains secure.

5 Oblivious Transfer Protocol from Semi-Commutative Masking

In this section we construct an OT protocol from a semi-commutative masking structure $\mathcal{M}$. We prove its UC security for passive adversaries with static corruptions in the $\mathcal{F}_{\mathsf{RO}}$-hybrid model assuming that $\mathcal{M}$ is $\mathsf{IND\text{-}Mask}$-secure and that the $\mathsf{ParallelEither}^{\mathcal{M}}$ problem is hard.

Motivation. Our OT protocol is inspired by the two-party Shamir three-pass protocol for secure message transmission shown in Figure 5a (ignoring the elements in square brackets), also known as the Massey-Omura encryption scheme. Here, Alice's input is a message g together with a secret mask a and Bob's input is another secret mask b. To transmit g, Alice first sends g^a to Bob who replies by masking it as g^{ab}. Now Alice removes her mask and replies with $g^{ab/a} = g^b$ to Bob who then inverts b and recovers g. This protocol can be modified to yield an OT protocol by including the elements in square brackets; this was proposed by Wu et al. [40].

Alice, acting as Sender, now has two inputs g_0 and g_1 and masks both with a to send g_0^a, g_1^a to Bob, the Receiver. In addition to his mask b, Bob now also has a choice bit $\mathsf{c} \in \{0, 1\}$ and he replies to Alice with $(g_\mathsf{c}^a)^b$. They then continue as before until Bob recovers g_c. The intuition for security is that the mask a cannot be deduced from either g_0^a or g_1^a and therefore the first message hides both of Alice's inputs from Bob. Also when Bob applies his own mask to one of the two messages, this hides his input bit c from Alice who does not know b.

Protocol Π^1_{OT}

PARAMETER: length n of the P_S's input strings.
SENDER'S INPUT: $\mathsf{m}_0, \mathsf{m}_1 \in \mathcal{M}_{\mathcal{E}}$.
RECEIVER'S INPUT: $\mathsf{c} \in \{0,1\}$.
COMMON INPUTS: Arbitrary $x_0 \neq x_1 \in X$ together with $r_0 \in R_{x_0}, r_1 \in R_{x_1}$ are shared and re-used for every instance of the protocol; an instance of the random oracle ideal functionality $\mathcal{F}_{\mathsf{RO}} : \{0,1\}^{\lambda} \to \mathcal{K}_{\mathcal{E}}$.

OT_1 **(Receiver 1)**

- Sample $\beta \xleftarrow{\$} M_B$ uniformly at random.
- Compute $r_{\mathsf{c}}^{\beta} := \beta(r_{\mathsf{c}})$ and $\beta^{-1} \in M_B$.
- Send r_{c}^{β} to P_S.

OT_2 **(Sender 1)**

- Sample $\alpha \xleftarrow{\$} M_A$ and compute $r_{\mathsf{b}}^{\alpha} := \alpha(r_{\mathsf{b}}) \in R_{x_{\mathsf{b}}^{\alpha}}$, $\mathsf{b} \in \{0,1\}$
- For $\mathsf{b} \in \{0,1\}$, call $\mathcal{F}_{\mathsf{RO}}$ twice on input x_{b}^{α} obtaining k_{b}, and compute $\mathsf{e}_{\mathsf{b}} \leftarrow \mathsf{Enc}(\mathsf{k}_{\mathsf{b}}, \mathsf{m}_{\mathsf{b}})$
- Compute $r_{\mathsf{c}}^{\alpha\beta} := \alpha(r_{\mathsf{c}}^{\beta})$
- Send $(r_{\mathsf{c}}^{\alpha\beta}, \mathsf{e}_0, \mathsf{e}_1)$ to P_R.

OT_3 **(Receiver 2)**

- Compute $r_{\mathsf{c}}^{\alpha} := \beta^{-1}(r_{\mathsf{c}}^{\alpha\beta})$ and $\mathsf{k}_R := \mathcal{F}_{\mathsf{RO}}(x_{\mathsf{c}}^{\alpha})$ where $r_{\mathsf{c}}^{\alpha} \in R_{x_{\mathsf{c}}^{\alpha}}$.
- Return $\mathsf{m}_{\mathsf{c}} := \mathsf{Dec}(\mathsf{k}_R, \mathsf{e}_{\mathsf{c}})$.

Fig. 6: The protocol Π^1_{OT} for realizing $\mathcal{F}_{\mathsf{OT}}$ from semi-commutative masking.

We remove the need to apply the inverse mask $1/a$ to g_{c}^{ab} since Alice's ignorance of c makes this impossible for general semi-commutative masking schemes due to the definition of inverse masks. In our new (discrete logarithm based) variant, the elements g_0 and g_1 are common to both parties. Rather than using a to send g_0^a, g_1^a to Bob (the Receiver), Alice (the Sender) does not go first. Instead, Bob first communicates his masked choice g_{c}^b, and then Alice applies her mask a and replies with g_{c}^{ab}. At that moment, she also computes g_0^a, g_1^a internally. She then uses these internal values to derive two symmetric keys k_0 and k_1. Those are used to encrypt Alice's actual OT inputs m_0 and m_1 as two ciphertexts e_0 and e_1 which she sends alongside g_{c}^{ab}. This allows Bob to recover g_{c}^a and hence decrypt e_{c} to recover m_{c}. As g_0 and g_1 are now established once and re-used for every instance of the protocol, this allows the flows to have only *two* passes rather than three. Figure 5b abstracts the symmetric encryption and only shows the flows that lead to Bob receiving the value g_{c}^a.

Construction. We now formally define our OT protocol from semi-commutative invertible masking schemes. Let $\mathcal{M} = \{X, R_X, [M_A, M_B, M_C]\}$ be an SCM structure with three masking sets; let $\mathcal{E} = \{(\mathsf{KGen}_{\mathcal{E}}, \mathsf{Enc}, \mathsf{Dec}), (\mathcal{K}_{\mathcal{E}}, \mathcal{M}_{\mathcal{E}}, \mathcal{C}_{\mathcal{E}})\}$ be a symmetric encryption scheme and let $\mathcal{F}_{\mathsf{RO}}$ be an instance of the RO ideal functionality with domain $\mathcal{D} = X$ and range $\mathcal{R} = \mathcal{K}_{\mathcal{E}}$. The protocol Π^1_{OT} is formally defined in Figure 6.

As described above, the idea of the protocol is that both the sender, P_S, and receiver, P_R, have as common input arbitrary elements $x_0 \neq x_1 \in X$ along with representations $r_0 \in R_{x_0}, r_1 \in R_{x_1}$. In the first pass, P_R takes a random mask $\beta \in M_B$ and sends $r_{\mathsf{c}}^{\beta} = \beta(r_{\mathsf{c}})$ to P_S, where c is its choice bit. In the second pass, P_S samples a random mask $\alpha \in M_A$ and computes $r_0^{\alpha} = \alpha(r_0)$ and $r_1^{\alpha} = \alpha(r_1)$. These elements uniquely determine $x_{\mathsf{b}}^{\alpha} \in X, \mathsf{b} \in \{0,1\}$. Thus the sender can compute two private keys $\mathsf{k_b}, \mathsf{b} \in \{0,1\}$ (by invoking twice the random oracle functionality $\mathcal{F}_{\mathsf{RO}}$ on input x_{b}^{α}) and encrypt its input messages $\mathsf{m}_0, \mathsf{m}_1$ accordingly. P_S then sends the ciphertexts $\mathsf{e_b} \leftarrow \mathsf{Enc}(\mathsf{k_b}, \mathsf{m_b}), \mathsf{b} \in \{0,1\}$, and $r_{\mathsf{c}}^{\alpha\beta} = \alpha(r_{\mathsf{c}}^{\beta})$ to P_R. The receiver has now all the information needed to recover the message $\mathsf{m_c}$ corresponding to its choice bit: it can apply the inverse β^{-1} to $r_{\mathsf{c}}^{\alpha\beta}$ using the semi-commutativity of $\mathcal{M}$, so that

$$\beta^{-1}(r_{\mathsf{c}}^{\alpha\beta}) = \beta^{-1}(\alpha(r_{\mathsf{c}}^{\beta})) = \beta^{-1}(\alpha(\beta(r_{\mathsf{c}}))) \in R_{x_{\mathsf{c}}^{\alpha}},$$

and recover $\mathsf{k_c} = \mathcal{F}_{\mathsf{RO}}(x_{\mathsf{c}}^{\alpha})$. This easily implies correctness of the scheme. Security is given by the following theorem. We give the proof in the full version and provide a sketch below.

Theorem 1. *The protocol Π_{OT}^1 of Figure 6 securely UC-realizes the functionality $\mathcal{F}_{\mathsf{OT}}$ of Figure 1 in the $\mathcal{F}_{\mathsf{RO}}$-hybrid model for semi-honest adversaries and static corruptions, under the assumption that $\mathcal{E}$ is IND-CPA-secure, that $\mathcal{M}$ is IND-Mask-secure and that the $\mathsf{ParallelEither}^{\mathcal{M}}$ problem is hard.*

Proof (sketch). We proceed by cases based on the honesty of each party. When both parties are corrupt, the simulator observes all the inputs and provides a perfect simulation. When only the receiver is corrupt, we build a reduction from a successful distinguishing environment first to the ParallelEither problem (by replacing $\mathsf{k}_{1-\mathsf{c}}$ with a random one) and then to the IND-CPA security of $\mathcal{E}$ (by replacing $\mathsf{m}_{1-\mathsf{c}}$ with a random one). When only the sender is corrupt we build a reduction to the IND-Mask security of $\mathcal{M}$. When no party is corrupt, we combine the two previous reductions to simulate a protocol transcript without knowledge of c, m_0 and m_1.

6 Active Secure Two-round OT from Commutative Masking

We now show how to compile our 2-round OT protocol Π_{OT}^1, described in Section 5, to a 2-round maliciously UC-secure protocol using the generic transformations introduced by Döttling et al. [18].

6.1 Additional OT Security Notions

A 2-round OT protocol with public setup consists of four algorithms (Setup, $\mathsf{OT}_1, \mathsf{OT}_2, \mathsf{OT}_3$) such that:

- $\mathsf{Setup}(1^{\lambda})$ generates a public input pin.

- $\mathsf{OT}_1(\mathsf{pin},\mathsf{c})$, where $\mathsf{c} \in \{0,1\}$ is the P_R choice bit, outputs $(\mathsf{st},\mathsf{ot}\_P_R)$
- $\mathsf{OT}_2(\mathsf{pin},\mathsf{ot}\_P_R,\mathsf{m}_0,\mathsf{m}_1)$, where $\mathsf{m}_0,\mathsf{m}_1$ are the sender's input messages, outputs ot_P_S
- $\mathsf{OT}_3(\mathsf{st},\mathsf{ot}\_P_S)$ outputs m_c

First we need to recall some security notions [18] for the receiver P_R and the sender P_S. The first definition states that P_S should not learn anything about P_R's choice bit c.

Definition 11 (Receiver's indistinguishability security). *For every PPT adversary $\mathcal{A}$:*

$$|\Pr[\mathcal{A}(\mathsf{pin},\mathsf{OT}_1(\mathsf{pin},0))=1]-\Pr[\mathcal{A}(\mathsf{pin},\mathsf{OT}_1(\mathsf{pin},1))=1]|=\mathsf{negl}(\lambda),$$

where pin *is the public output of the setup phase.*

The next definition concerns the security of the sender; it states that P_R cannot compute both secret values y_0 and y_1 used by OT_2 to protect m_0 and m_1, but not necessarily in the same experiment.

Definition 12 (Sender's search security). *Let $\mathcal{A}=(\mathcal{A}_1,\mathcal{A}_2)$ be an adversary where $\mathcal{A}_2$ outputs a string y^*. Consider the following experiment $\mathsf{Exp}_{\mathsf{sOT}}^{\mathsf{pin},\rho,w}(\mathcal{A})$, indexed by a pin, random coins $\rho \in \{0,1\}^\lambda$ and a bit $w \in \{0,1\}$.*

1. *Run $(\mathsf{ot}\_P_R,\mathsf{st}) \leftarrow \mathcal{A}_1(1^\lambda,\mathsf{pin};\rho)$.*
2. *Compute $(\mathsf{ot}\_P_S,\mathsf{y}_0,\mathsf{y}_1) \overset{\$}{\leftarrow} \mathsf{OT}_2(\mathsf{pin},\mathsf{ot}\_P_R)$.*
3. *Run $\mathsf{y}^* \leftarrow \mathcal{A}_2(\mathsf{st},\mathsf{ot}\_P_S,w)$ and output 1 iff $\mathsf{y}^*=\mathsf{y}_w$.*

We say that $\mathcal{A}$ breaks a scheme's Sender's search (sOT) security *if there exists a non-negligible function ϵ such that*

$$\Pr_{\mathsf{pin},\rho}[\Pr[\mathsf{Exp}_{\mathsf{sOT}}^{\mathsf{pin},\rho,0}(\mathcal{A})=1]>\epsilon \text{ and } \Pr[\mathsf{Exp}_{\mathsf{sOT}}^{\mathsf{pin},\rho,1}(\mathcal{A})=1]>\epsilon]>\epsilon,$$

where $\mathsf{pin} \overset{\$}{\leftarrow} \mathsf{Setup}$ and $\rho \overset{\$}{\leftarrow} \{0,1\}^\lambda$.

6.2 Two rounds OT with Active UC-Security

We provide an intermediary result which enables us to use the general compiler from [18] to get an actively secure 2-round OT protocol starting from $\mathit{\Pi}_{\mathsf{OT}}^1$. First we introduce and discuss a new security assumption derived from the $\mathsf{Parallel}$ problem but more suited to active adversaries. Then we show that our protocol satisfies the security notions of Definitions 11 and 12. Finally, by applying the general transformations from sOT to UC OT described in [18], we obtain a fully UC-secure two-round OT protocol. We note that we are able to remove the random oracle from our protocol to achieve sOT security; therefore the resulting OT protocol requires only the CRS. We define our new computational problem as follows.

Definition 13 ($\mathsf{ParallelDouble}$)**.** *Given* $(i, j, r, r_{x_0}, r_{x_1}, r_y)$ *with the promise that* $i \neq j$ *and that* $r_{x_\mathsf{b}} = \mu_{x_\mathsf{b}}(r)$, $\mathsf{b} \in \{0, 1\}$ *and* $r_y = \mu_y(r)$ *for random* $\mu_{x_\mathsf{b}} \xleftarrow{\$} M_i$ *and* $\mu_y \xleftarrow{\$} M_j$*, and given a* one-time *access to an oracle* $\mathcal{O}_y$ *which, when given* $r \in R$ *returns* $\mu_y(r)$*, compute* $z_0, z_1 \in X$ *such that* both $\mu_{x_\mathsf{b}}(r_y) \in R_{z_\mathsf{b}}$.

The instantiation of this problem in the discrete logarithm case is, when given (g, g^a, g^b, g^c) and a one-time access to an exponentiation-by-c oracle, to return both g^{ac} and g^{bc}. For practical efficiency, it is also desirable that g^a and g^b remain constant across multiple instances of the $\mathsf{ParallelDouble}$ problem, with only g^c being randomly sampled in each instance. This version of the problem is similar to the one-more static CDH problem where an adversary has to successfully compute one more CDH challenge than it was able to ask from a helper oracle [9].

Security of the $\mathit{\Pi}^1_{\mathsf{OT}}$ *protocol.* We then prove that protocol $\mathit{\Pi}^1_{\mathsf{OT}}$ achieves Receiver's indistinguishability and Sender's search security.

Proposition 1. *The protocol* $\mathit{\Pi}^1_{\mathsf{OT}}$ *in Figure 6 satisfies computational receiver's indistinguishability security and sender's* sOT *security under the assumption that* $\mathcal{M}$ *is* $\mathsf{IND\text{-}Mask}$*-secure and that the* $\mathsf{ParallelDouble}^{\mathcal{M}}$ *problem is hard.*

Proof. Receiver's indistinguishability follows from the $\mathsf{IND\text{-}Mask}$-security assumption. By setting the public inputs r_0 and r_1 in $\mathit{\Pi}^1_{\mathsf{OT}}$ as they are computed in the $\mathsf{IND\text{-}Mask}$ experiment, the random mask μ is distributed in the same way as the mask β in OT_1. Therefore if an adversary breaks the receiver's indistinguishability for $\mathit{\Pi}^1_{\mathsf{OT}}$, this can be reduced to a solution to the $\mathsf{IND\text{-}Mask}$ problem.

Sender's search security. To prove sOT security for $\mathit{\Pi}^1_{\mathsf{OT}}$ we assume the existence of an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ and a non-negligible ϵ such that

$$\Pr_{\mathsf{pin},\rho}[\Pr[\mathsf{Exp}^{\mathsf{pin},\rho,0}_{\mathsf{sOT}}(\mathcal{A}) = 1] > \epsilon \text{ and } \Pr[\mathsf{Exp}^{\mathsf{pin},\rho,1}_{\mathsf{sOT}}(\mathcal{A}) = 1] > \epsilon] > \epsilon,$$

and we build a reduction $\mathcal{B}$ that is given a $\mathsf{ParallelDouble}$ challenge $(i, j, r, r_{x_0}, r_{x_1}, r_y)$ with access to an oracle $\mathcal{O}_y$ (Definition 13). Instead of running Setup to generate r_0 and r_1, $\mathcal{B}$ sets $r_0 \leftarrow r_{x_0}$ and $r_1 \leftarrow r_{x_1}$; also $\mathcal{B}$ samples $\rho \xleftarrow{\$} \{0, 1\}^\lambda$. As this ensures that pin is distributed identically to the output of Setup, pin and ρ are good for $\mathcal{A}$ with probability at least ϵ.

After $\mathcal{B}$ runs $\mathcal{A}_1$, which outputs $(\mathsf{ot\_}P_R, \mathsf{st})$, it queries the oracle to obtain $\mathsf{ot\_}P_{S,0} \leftarrow \mathcal{O}_y(\mathsf{ot\_}P_R)$. It also computes $\mathsf{ot\_}P_{S,1} \leftarrow \mu(\mathsf{ot\_}P_{S,0})$ for a random $\mu \in M_k$ with $i \neq k \neq j$; it also computes μ^{-1}. Then, for $w \in \{0, 1\}$, $\mathcal{B}$ runs $\mathsf{y}^*_w \leftarrow \mathcal{A}_2(\mathsf{st}, \mathsf{ot\_}P_{S,w}, w)$ and updates $\mathsf{y}^*_1 \leftarrow \mu^{-1}(\mathsf{y}^*_1)$. Finally $\mathcal{B}$ returns y^*_0 and the updated y^*_1 as the $\mathsf{ParallelDouble}$ answer.

Since $\Pr[\mathsf{Exp}^{\mathsf{pin},\rho,0}_{\mathsf{sOT}}(\mathcal{A}) = 1] > \epsilon$ and $\Pr[\mathsf{Exp}^{\mathsf{pin},\rho,1}_{\mathsf{sOT}}(\mathcal{A}) = 1] > \epsilon$, with probability ϵ^2, $\mathcal{A}_2$ is successful for both inputs $(\mathsf{st}, \mathsf{ot\_}P_{S,0}, 0)$ and $(\mathsf{st}, \mathsf{ot\_}P_{S,1}, 1)$ as the two messages are made independent by $\mathcal{B}$'s addition of μ. If this happens, then y^*_0 is exactly one of the answers, and the update of y^*_1 by $\mathcal{B}$ removes the extra mask μ and means that y^*_1 is then the other answer to the $\mathsf{ParallelDouble}$ problem. Hence $\mathcal{B}$ is successful with probability at least ϵ^3.

Theorem 2. *Under the assumption that $\mathcal{M}$ is* $\mathsf{IND\text{-}Mask}$*-secure and that the* $\mathsf{ParallelDouble}^{\mathcal{M}}$ *problem is hard, there exists a 2-round UC-secure OT protocol constructed from* Π^1_{OT}.

Proof. This follows from the transformations and results of [18, Theorems 8, 9, 11, 12, 14, 19 and 21].

Corollary 1. *By instantiating the semi-commutative masking scheme, there exists an actively secure 2-round OT protocol based on supersingular isogenies.*

We remark here that the isogeny-based OT protocols proposed by Vitse [38], while being semantically secure against malicious adversaries, require three rounds of communication; this implies that they cannot be transformed to achieve two-round OT with fully UC-security using the work of Döttling et al.

Acknowledgements

This work has been supported in part by ERC Advanced Grant ERC-2015-AdG-IMPaCT, by CyberSecurity Research Flanders with reference number VR20192203, by the Defense Advanced Research Projects Agency (DARPA) and Space and Naval Warfare Systems Center, Pacific (SSC Pacific) under contracts No. N66001-15-C-4070 and No. HR001120C0085, by the FWO under an Odysseus project GOH9718N and by EPSRC grant EP/S01361X/1

References

1. Adj, G., Ahmadi, O., Menezes, A.: ON ISOGENY GRAPHS OF SUPERSINGULAR ELLIPTIC CURVES OVER FINITE FIELDS. Cryptology ePrint Archive, Report 2018/132 (2018), https://eprint.iacr.org/2018/132
2. Azarderakhsh, R., Jalali, A., Jao, D., Soukharev, V.: Practical supersingular isogeny group key agreement. Cryptology ePrint Archive, Report 2019/330 (2019), https://eprint.iacr.org/2019/330
3. Azarderakhsh, R., Jao, D., Kalach, K., Koziel, B., Leonardi, C.: Key compression for isogeny-based cryptosystems. In: Emura, K., Hanaoka, G., Zhang, R. (eds.) Proceedings of the 3rd ACM International Workshop on ASIA Public-Key Cryptography, APKC. pp. 1–10. ACM (2016)
4. Barreto, P., Oliveira, G., Benits, W.: Supersingular isogeny oblivious transfer. Cryptology ePrint Archive, Report 2018/459 (2018), https://eprint.iacr.org/2018/459
5. Barreto, P.S.L.M., David, B., Dowsley, R., Morozov, K., Nascimento, A.C.A.: A framework for efficient adaptively secure composable oblivious transfer in the ROM. Cryptology ePrint Archive, Report 2017/993 (2017), http://eprint.iacr.org/2017/993
6. Brakerski, Z., Döttling, N.: Two-message statistically sender-private OT from LWE. In: Beimel, A., Dziembowski, S. (eds.) TCC 2018, Part II. LNCS, vol. 11240, pp. 370–390. Springer, Heidelberg (Nov 2018)

7. Branco, P., Ding, J., Goulão, M., Mateus, P.: A framework for universally composable oblivious transfer from one-round key-exchange. In: Albrecht, M. (ed.) 17th IMA International Conference on Cryptography and Coding. LNCS, vol. 11929, pp. 78–101. Springer, Heidelberg (Dec 2019)
8. Branco, P., Ding, J., Goulão, M., Mateus, P.: A framework for universally composable oblivious transfer from one-round key-exchange. Cryptology ePrint Archive, Report 2019/726 (2019), https://eprint.iacr.org/2019/726. To appear at the 17th IMA International Conference on Cryptography and Coding.
9. Bresson, E., Monnerat, J., Vergnaud, D.: Separation results on the "one-more" computational problems. In: Malkin, T. (ed.) CT-RSA 2008. LNCS, vol. 4964, pp. 71–87. Springer, Heidelberg (Apr 2008)
10. Byali, M., Patra, A., Ravi, D., Sarkar, P.: Fast and universally-composable oblivious transfer and commitment scheme with adaptive security. Cryptology ePrint Archive, Report 2017/1165 (2017), https://eprint.iacr.org/2017/1165
11. Canetti, R.: Universally composable security: A new paradigm for cryptographic protocols. In: 42nd FOCS. pp. 136–145. IEEE Computer Society Press (Oct 2001)
12. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: An efficient post-quantum commutative group action. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018, Part III. LNCS, vol. 11274, pp. 395–427. Springer, Heidelberg (Dec 2018)
13. Childs, A., Jao, D., Soukharev, V.: Constructing elliptic curve isogenies in quantum subexponential time. Journal of Mathematical Cryptology 8(1), 1–29 (2014), a pre-print version appears at https://arxiv.org/abs/1012.4019
14. Chou, T., Orlandi, C.: The simplest protocol for oblivious transfer. In: Lauter, K.E., Rodríguez-Henríquez, F. (eds.) LATINCRYPT 2015. LNCS, vol. 9230, pp. 40–58. Springer, Heidelberg (Aug 2015)
15. Costello, C., Longa, P., Naehrig, M.: Efficient algorithms for supersingular isogeny Diffie-Hellman. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part I. LNCS, vol. 9814, pp. 572–601. Springer, Heidelberg (Aug 2016)
16. Couveignes, J.M.: Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291 (2006), http://eprint.iacr.org/2006/291
17. De Feo, L., Jao, D., Plût, J.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Journal of Mathematical Cryptology 8(3), 209–247 (2014), a pre-print version appears at https://eprint.iacr.org/2011/506
18. Döttling, N., Garg, S., Hajiabadi, M., Masny, D., Wichs, D.: Two-round oblivious transfer from CDH or LPN. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part II. LNCS, vol. 12106, pp. 768–797. Springer, Heidelberg (May 2020)
19. Faz-Hernández, A., López, J., Ochoa-Jiménez, E., Rodríguez-Henríquez, F.: A faster software implementation of the supersingular isogeny diffie-hellman key exchange protocol. IEEE Transactions on Computers 67(11), 1622–1636 (Nov 2018)
20. Fujioka, A., Takashima, K., Terada, S., Yoneyama, K.: Supersingular isogeny Diffie-Hellman authenticated key exchange. In: Lee, K. (ed.) ICISC 18. LNCS, vol. 11396, pp. 177–195. Springer, Heidelberg (Nov 2019)
21. Fujioka, A., Takashima, K., Yoneyama, K.: One-round authenticated group key exchange from isogenies. In: Steinfeld, R., Yuen, T.H. (eds.) ProvSec 2019. LNCS, vol. 11821, pp. 330–338. Springer, Heidelberg (Oct 2019)
22. Galbraith, S.: Isogeny crypto. Blog post from ellipticnews (2019), https://ellipticnews.wordpress.com/2019/11/09/isogeny-crypto/, last accessed Apr 15, 2020

23. Galbraith, S.D., Petit, C., Shani, B., Ti, Y.B.: On the security of supersingular isogeny cryptosystems. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part I. LNCS, vol. 10031, pp. 63–91. Springer, Heidelberg (Dec 2016)
24. Galbraith, S.D., Petit, C., Silva, J.: Identification protocols and signature schemes based on supersingular isogeny problems. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017, Part I. LNCS, vol. 10624, pp. 3–33. Springer, Heidelberg (Dec 2017)
25. Galbraith, S.D., Vercauteren, F.: Computational problems in supersingular elliptic curve isogenies. Quantum Information Processing 17(10), 265 (Aug 2018), https://doi.org/10.1007/s11128-018-2023-6
26. Goldreich, O., Oren, Y.: Definitions and properties of zero-knowledge proof systems. Journal of Cryptology 7(1), 1–32 (Dec 1994)
27. Jao, D., De Feo, L.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: Yang, B.Y. (ed.) Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011. pp. 19–34. Springer, Heidelberg (Nov / Dec 2011)
28. Keller, M., Orsini, E., Scholl, P.: MASCOT: Faster malicious arithmetic secure computation with oblivious transfer. In: Weippl, E.R., Katzenbeisser, S., Kruegel, C., Myers, A.C., Halevi, S. (eds.) ACM CCS 2016. pp. 830–842. ACM Press (Oct 2016)
29. Kutas, P., Martindale, C., Panny, L., Petit, C., Stange, K.E.: Weak instances of sidh variants under improved torsion-point attacks. Cryptology ePrint Archive, Report 2020/633 (2020), https://eprint.iacr.org/2020/633
30. Lai, Y.F., Galbraith, S.D., Delpech de Saint Guilhem, C.: Compact, efficient and uc-secure isogeny-based oblivious transfer. Cryptology ePrint Archive, Report 2020/1012 (2020), https://eprint.iacr.org/2020/1012
31. Nielsen, J.B., Nordholt, P.S., Orlandi, C., Burra, S.S.: A new approach to practical active-secure two-party computation. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 681–700. Springer, Heidelberg (Aug 2012)
32. Peikert, C., Vaikuntanathan, V., Waters, B.: A framework for efficient and composable oblivious transfer. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 554–571. Springer, Heidelberg (Aug 2008)
33. Petit, C.: Faster algorithms for isogeny problems using torsion point images. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017, Part II. LNCS, vol. 10625, pp. 330–353. Springer, Heidelberg (Dec 2017)
34. Rabin, M.O.: How to exchange secrets by oblivious transfer. Technical Report TR-81, Aiken Computation Laboratory, Harvard University (1981)
35. Sahu, R.A., Gini, A., Pal, A.: Supersingular isogeny-based designated verifier blind signature. Cryptology ePrint Archive, Report 2019/1498 (2019), https://eprint.iacr.org/2019/1498
36. Silverman, J.H.: The arithmetic of elliptic curves, Graduate Texts in Mathematics, vol. 106. Springer Science & Business Media (1986)
37. Urbanick, D., Jao, D.: Sok: The problem landscape of sidh. In: APKC'18: Proceedings of the 5th ACM on ASIA Public-Key Cryptography Workshop. pp. 53–60. ACM (2018)
38. Vitse, V.: Simple oblivious transfer protocols compatible with supersingular isogenies. In: Buchmann, J., Nitaj, A., eddine Rachidi, T. (eds.) AFRICACRYPT 19. LNCS, vol. 11627, pp. 56–78. Springer, Heidelberg (Jul 2019)
39. Wang, X., Ranellucci, S., Katz, J.: Global-scale secure multiparty computation. In: Thuraisingham, B.M., Evans, D., Malkin, T., Xu, D. (eds.) ACM CCS 2017. pp. 39–56. ACM Press (Oct / Nov 2017)

40. Wu, Q.H., Zhang, J.H., Wang, Y.M.: Practical t-out-n oblivious transfer and its applications. In: Qing, S., Gollmann, D., Zhou, J. (eds.) ICICS 03. LNCS, vol. 2836, pp. 226–237. Springer, Heidelberg (Oct 2003)