# Simple oblivious transfer protocols compatible with Kummer and supersingular isogenies

Vanessa Vitse

Univ. Grenoble Alpes, CNRS, Institut Fourier, F-38000 Grenoble, France

**Abstract.** The key exchange protocol of Diffie and Hellman, which can be defined for any group, has the special feature of using only exponentiations. In particular, it can also be instantiated in Kummer varieties, which are not groups, and in the post-quantum isogeny-based setting, with the supersingular isogeny DH scheme of De Feo, Jao and Plût (SIDH).

In this article, we propose a new simple oblivious transfer (OT) protocol, based on the Diffie-Hellman key exchange, that only uses exponentiations; we also revisit the older Wu-Zhang-Wang scheme. Both protocols can be directly instantiated on fast Kummer varieties; more importantly, they can also be transposed in the post-quantum SIDH setting. The security of our proposals relies on the hardness of non-standard versions of the (supersingular) Diffie-Hellman problem, that are investigated within this article. To the best of our knowledge, these protocols are the simplest secure discrete-log based OT schemes using only exponentiations, and the first isogeny-based OT schemes.

**Keywords:** Oblivious transfer, Diffie-Hellman key exchange, supersingular isogeny, post-quantum cryptography

## 1 Introduction

The key exchange protocol of Diffie and Hellman [13] is undoubtedly the single most influential concept in the history of modern cryptography, and though more than forty years old, it continues to see new developments. A convenient feature of the Diffie-Hellman protocol is that it can be instantiated in any group, provided that the discrete logarithm problem (DLP) is hard; current applications no longer use the multiplicative group of finite fields where it was first defined but rather the group of points of an elliptic curve or Jacobian variety. Interestingly, the key exchange does not use group products, but only *exponentiations*, or more precisely commuting exponentiation maps. This seemingly benign observation actually allows the generalization of the Diffie-Hellman protocol to group-less settings, two of which we will describe now.

The first one is Kummer varieties, which are formed from Jacobian varieties by identifying a point and its inverse. A Kummer variety is not a group, but nevertheless inherits some of the operations of its parent Jacobian: in particular, there are well-defined (in additive notations) multiplication maps $[D] \mapsto [a\,D]$

and differential addition $\{[D], [D']\} \mapsto \{[D + D'], [D - D']\}$. These operations are sufficient for implementing the Diffie-Hellman key exchange, and more importantly, they are usually faster than their Jacobian counterparts. For elliptic curves, it corresponds to the famous $x$-only Montgomery's ladder [23]. The use of Kummer varieties in higher genus is more recent (see notably [16,17]), and their performances in genus 2 make them competitive alternatives to elliptic curves [4,29].

The second setting is supersingular isogeny graphs. A drawback of the Diffie-Hellman protocol is its vulnerability to quantum attacks: if quantum computers are eventually constructed, they will be able to efficiently solve the discrete logarithm problem thanks to Shor's algorithm [31]. For this reason, there have been in recent years a push toward the conception of efficient, quantum-resistant cryptographic schemes. One such proposal is the SIDH key exchange of De Feo, Jao and Plût [12], which is directly adapted from Diffie-Hellman: the group of points of a single elliptic curve is replaced by the set of all supersingular elliptic curves defined over a finite field $\mathbb{F}_{p^2}$, and exponentiation maps are replaced by isogenies of prescribed degrees. In this context, the analog of the discrete logarithm problem is the *computational supersingular isogeny problem*: given two supersingular elliptic curves $E$ and $E'$, find an isogeny $\phi$ from $E$ to $E'$. There is currently no known subexponential quantum algorithm for solving this problem.

The analogy between the group setting and the supersingular isogeny setting is far from being an exact correspondence, however. Consequently, the adaptation of a DLP-based protocol using only exponentiations to this second setting can be quite challenging (while on the other hand, the adaptation to Kummer varieties is trivial). Nevertheless, we believe that most exponentiation-only DLP-based protocols can be modified to work with supersingular isogenies. The goal of this article is to demonstrate this claim on two examples: the first is a new oblivious transfer protocol, while the second is an older scheme of Wu, Zhang and Wang. Both protocols are exponentiation-only, and we explain how to convert them into SIDH-based protocols. A last, marginal example is the construction of a signature scheme for the – unlikely to exist – "gap" supersingular case.

Oblivious transfer is among the fundamental tools of cryptography. It can be presented quite simply: Alice knows two secrets, say $s_0$ and $s_1$. Bob wants to know one of these secrets, but he does not want Alice to know which one. Oblivious transfer protocols (more precisely here, $\binom{2}{1}$-oblivious tranfer) resolve exactly that, allowing Bob to learn the secret of his choice without learning anything about the other secret, and without divulging anything about his choice to Alice[1]. Introduced by Rabin [28] and Even et al. [14] in the early 80's, oblivious transfer is a universal basic block for secure multiparty computations [20], and a number of constructions have been proposed. In many protocols, the security relies on the computational hardness of either the RSA problem or the Diffie-Hellman problem, or variants thereof. In this article, we are interested

[1] This is usually not meant in a information-theoretic sense, but rather in a computational-theoretic one.

in the latter (DH-based protocols); the most well-known are Bellare-Micali's, Naor-Pinkas's and Chou-Orlandi's [3,10,24]. To the best of our knowledge, only Wu, Zhang and Wang's construction [37] relies solely on exponentiations, but it requires additional validation measures to be secure, see Sect. 2.2. And while several post-quantum OT schemes have been proposed (most notably by Peikert et al. [26]; see also [19] for more references), none of them are based on supersingular isogenies.

The first contribution of this article is the study and construction of DH-based oblivious transfer schemes that use only exponentiations (Sect. 2). We begin by reviewing the protocol of Wu, Zhang and Wang [37], explaining how to improve its security. We then propose a new, conceptually simple oblivious transfer scheme. Because it can be straightforwardly adapted to work on fast Kummer varieties, we believe this protocol to be interesting on its own, outside of the post-quantum setting. For its analysis (Sect. 2.4 and 2.5), we define a notion of semantic security of an oblivious transfer scheme, capturing the computational intractability for the receiver of gaining information on both of Alice's secrets. The security of our new protocol relies on the hardness of a new variant of the Diffie-Hellman problem, in computational form if the underlying encryption scheme is modeled as a random oracle, and in decisional form if it satisfies the IND-CPA property. We also analyse Wu-Zhang-Wang protocol, showing that in the random oracle model (and only in this model), its security is equivalent to the hardness of a second variant of the Diffie-Hellman problem. Of course, these two problems deserve more scrutiny, but we give some arguments in favor of their intractability, proving in Appendix A that the first one is basically as hard as the discrete logarithm problem in the generic group model.

We recall in the next section the supersingular isogeny Diffie-Hellman key exchange (SIDH) of De Feo, Jao and Plût, before presenting in Sect. 4.2 the corresponding version of our new OT protocol. We also explain how to translate Wu-Zhang-Wang protocol in this new setting, raising some interesting open problems along the way. The last section deals with their security, which mainly relies on the hardness of the isogeny versions of the previous problems. However, it also requires the hardness of the (extended) decisional supersingular isogeny problem, which has no equivalent for groups. We show in Appendix B that it would be possible to mimic the construction of short signatures for gap Diffie-Hellman groups and obtain a simple post-quantum isogeny-based signature scheme, in the unlikely event that this DSSI problem turned out to be easy.

## 2 Simple Diffie-Hellman based oblivious transfer protocols

### 2.1 The Diffie-Hellman key exchange

In the standard Diffie-Hellman key exchange protocol, the two participants Alice and Bob, who communicate through an insecure communication channel, agree on a cyclic group $G$ and a generator $g$ of $G$. Alice and Bob both choose secret integers $a$ and $b$ respectively; Alice computes $A = g^a$ via a fast exponentiation algorithm and sends it to Bob, while Bob computes and sends Alice $B = g^b$. Upon reception of $A$, resp. $B$, Bob computes $A^b$, resp. Alice computes $B^a$. Of course, $A^b = (g^a)^b = g^{ab} = (g^b)^a = B^a$, thus Alice and Bob now have a shared secret from which they can derive an actual key for encrypting securely their future communications.

$$\begin{tikzcd}
& A = g^a \arrow[dr, "\phi_b"] & \\
g \arrow[ur, "\phi_a"] \arrow[dr, "\phi_b"'] & & (g^a)^b = (g^b)^a \\
& B = g^b \arrow[ur, "\phi_a"'] &
\end{tikzcd}$$

**Fig. 1.** Another view of the Diffie-Hellman key exchange.

Another point of view on this protocol is the following (see Fig. 1): Alice has a secret map $\phi_a : G \to G$, $x \mapsto x^a$, and Bob has his own secret map $\phi_b : x \mapsto x^b$. Both apply their secret map to a common starting element $g \in G$, then to the value computed by the other participant. The fact that they obtain the same final value comes from the commutativity property $\phi_a \circ \phi_b = \phi_b \circ \phi_a$. Of course, their maps remain secret even if $\phi_a(g)$ and $\phi_b(g)$ are known, precisely because the discrete log problem is hard in $G$.

Since this scheme only uses exponentiations in $G$ and no multiplication, it has been applied succesfully to Kummer varieties [16,17,29], which only form a "pseudo-group". This property is also what will enable its transposition to the quantum-resistant isogeny setting, see Sect. 3.

Because of its simplicity, the Diffie-Hellman key exchange has served as a basis for several oblivious transfer methods, most notably by Bellare and Micali, Naor and Pinkas, and more recently Chou and Orlandi [3,10,24]. However, all these schemes use some multiplications in the group $G$, besides exponentiations. To the best of our knowledge, the only existing exponentiation-only oblivious transfer construction is the 2003 protocol of Wu, Zhang and Wang [37]. We revisit this protocol in the next section, before proposing in Sect. 2.3 a new scheme, conceptually close to Bellare and Micali's (and Chou and Orlandi's variant). Being based uniquely on exponentiations, both protocols can be adapted to work directly on fast Kummer varieties, and we will be able in Sect. 4 to turn them into quantum-resistant, isogeny-based protocols.

### 2.2 The oblivious transfer protocol of Wu, Zhang and Wang

In the oblivious transfer setting, Alice has two secrets $s_0, s_1$ and Bob wants to learn one of them, without allowing Alice to know which one; and Alice does not want Bob to learn both secrets. Let $k \in \{0, 1\}$ be the index of Bob's choice. As published in [37], Wu-Zhang-Wang protocol requires Alice's secrets to be (encoded as) elements of the group $G$. It is based on the "double lock" principle, which in turn amounts to the commutativity of the exponentiation maps.

1. Setup: Alice and Bob agree on a cyclic group $G$ of prime order and a generator $g$ of $G$, such that the discrete logarithm problem (and the Diffie-Hellman problem) is hard in $G$. They also agree on a method to encode messages as elements of $G$.
2. Alice picks a uniformly random integer $a \in \{1, \dots, \#G - 1\}$. She computes $A_0 = (s_0)^a$ and $A_1 = (s_1)^a$ and sends them to Bob.
3. Bob chooses a uniformly random integer $b \in \{1, \dots, \#G - 1\}$. According to the index $k$ of the secret he is interested in, he computes the group element $B' = (A_k)^b$ and sends it to Alice.
4. Alice computes $B = (B')^{a^{-1}}$ and sends it to Bob.
5. Bob computes $B^{b^{-1}}$.

Here $a^{-1}$ and $b^{-1}$ stand for the inverses of $a$ and $b$ modulo $\#G$. Basically, Alice has "locked" her secrets using exponention by $a$, Bob adds his lock (exponentiation by $b$) on one of them, then Alice removes her lock, and finally Bob unlocks his desired secret. Correctness of the protocol follows from the identity $B^{b^{-1}} = ((((s_k)^a)^b)^{a^{-1}})^{b^{-1}} = s_k$. As above, it can be interpreted in terms of the commutativity of the maps $\phi_a$, $\phi_b$ and their inverses; see Fig. 2.

$$\begin{tikzcd}
 & A_0 = (s_0)^a \arrow[rrd, bend left, "\phi_b"] & & \\
s_0 \arrow[ru, "\phi_a"] & & A_1 = (s_1)^a & \\
 & s_1 \arrow[ru, "\phi_a"] & & B' = (s_0)^{ab} \arrow[ld, "\phi_a^{-1}"] \\
 & & B = (s_0)^b \arrow[llu, bend left, "\phi_b^{-1}"] &
\end{tikzcd}$$

$$\begin{tikzcd}
 & A_0 = (s_0)^a & & \\
s_0 \arrow[ru, "\phi_a"] & & A_1 = (s_1)^a \arrow[rd, "\phi_b"] & \\
 & s_1 \arrow[ru, "\phi_a"] & & B' = (s_1)^{ab} \arrow[ld, "\phi_a^{-1}"] \\
 & & B = (s_1)^b \arrow[lu, "\phi_b^{-1}"] &
\end{tikzcd}$$

**Fig. 2.** Wu-Zhang-Wang protocol (left, $k = 0$; right, $k = 1$).

Unfortunately, this protocol is unsecure against a malicious Bob (we will give more complete definitions in the security review of Sect. 2.5). Indeed, a dishonest

Bob can send $B'' = (A_0^x A_1^y)^b$ for some $x, y$ of his choice to Alice, instead of $A_0^b$ or $A_1^b$. If he does that, at the end of the exchange he will learn not $s_0$ nor $s_1$, but something related to both, typically their quotient $s_0/s_1$. A way to prevent this is to use a validation method, as discussed in [37], in order to ensure that Bob sends either $A_0^b$ or $A_1^b$, but this adds to the complexity of the protocol.

A more interesting possibility is to turn the protocol into a *random* oblivious transfer [2]. Instead of $s_0$ and $s_1$, Alice starts with two random elements $r_0$ and $r_1$ of $G$, and computes $A_0$ and $A_1$ as $(r_0)^a$ and $(r_1)^a$. At the end of the exchange, Bob knows either $r_0$ and $r_1$, but not both, and Alice does not know which one; at this point her secrets $s_0$ and $s_1$ have not been involved yet. Then $r_0$ and $r_1$ can be used as key seeds to encrypt $s_0$ and $s_1$ using a symmetric encryption function. If it is secure enough, a malicious Bob could still learn $r_0^x r_1^y$ instead of $r_0$ or $r_1$, but that does not help him decrypt Alice's secrets. We give below the complete protocol.; it is summed up in Fig. 3.

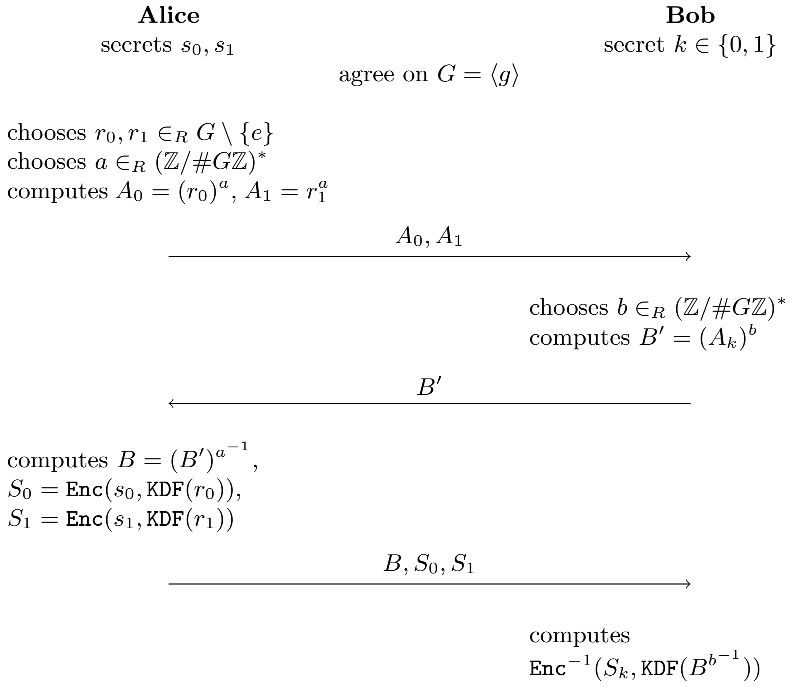
**Alice**
secrets $s_0, s_1$
**Bob**
secret $k \in \{0, 1\}$
agree on $G = \langle g \rangle$
chooses $r_0, r_1 \in_R G \setminus \{e\}$
chooses $a \in_R (\mathbb{Z}/\#G\mathbb{Z})^*$
computes $A_0 = (r_0)^a$, $A_1 = r_1^a$
$A_0, A_1$
chooses $b \in_R (\mathbb{Z}/\#G\mathbb{Z})^*$
computes $B' = (A_k)^b$
$B'$
computes $B = (B')^{a^{-1}}$,
$S_0 = \mathtt{Enc}(s_0, \mathtt{KDF}(r_0))$,
$S_1 = \mathtt{Enc}(s_1, \mathtt{KDF}(r_1))$
$B, S_0, S_1$
computes
$\mathtt{Enc}^{-1}(S_k, \mathtt{KDF}(B^{b^{-1}}))$

**Fig. 3.** Random OT version of Wu-Zhang-Wang protocol.

1. Setup: Alice and Bob agree on a cyclic group $G$ of prime order, such that the discrete logarithm problem (and the Diffie-Hellman problem) is hard in $G$. They also agree on a symmetric encryption scheme `Enc` and a key derivation function `KDF`.

2. Alice picks two uniformly random, non-neutral elements $r_0, r_1 \in G$, and a uniformly random integer $a \in \{1, \dots, \#G - 1\}$. She computes $A_0 = (r_0)^a$ and $A_1 = (r_1)^a$ with a fast exponentiation algorithm and sends them to Bob.
3. Bob chooses a uniformly random integer $b \in \{1, \dots, \#G - 1\}$. According to the index $k$ of the secret he is interested in, he computes the group element $B' = (A_k)^b$ and sends it to Alice.
4. Alice encrypts her secrets $s_0$ and $s_1$ with the key derived from the random values $r_0$ and $r_1$ respectively. She computes $B = (B')^{a^{-1}}$ and sends it to Bob, together with the ciphertexts $S_0 = \texttt{Enc}(s_0, \texttt{KDF}(r_0))$ and $S_1 = \texttt{Enc}(s_1, \texttt{KDF}(r_1))$.
5. Bob decrypts $S_k$ with the key derived from $B^{b^{-1}} = r_k$.

### 2.3 A new, simple DH-based oblivious transfer protocol

We propose in this section a new random oblivious transfer protocol, also based on the Diffie-Hellman key exchange scheme. We will see that it has some advantages compared to Wu-Zhang-Wang protocol, with respect to security (Sect. 2.5) and complexity in the supersingular isogeny setting (Sect. 4.3).

As above, Alice has two secrets $s_0, s_1$ and Bob wants to learn one of them, without allowing Alice to know which one; and Alice does not want Bob to learn both secrets. The index of Bob's choice is denoted by $k \in \{0, 1\}$.

1. Setup: Alice and Bob agree on a cyclic group $G$ of prime order and a generator $g$ of $G$, such that the discrete logarithm problem (and the Diffie-Hellman problem) is hard in $G$. They also agree on a secure symmetric encryption function $\texttt{Enc}$ and key derivation function $\texttt{KDF}$.
2. – Alice picks two different integers $a_0, a_1 \in \{1, \dots, \#G - 1\}$, chosen independently and uniformly randomly.
   – For each $i \in \{0, 1\}$, she computes with a fast exponentiation algorithm $A_i = g^{a_i}$; she sends Bob $A_0, A_1$.
3. Bob chooses a uniformly random integer $b \in \{1, \dots, \#G - 1\}$.
   – He computes the group element $B = g^b$.
   – According to the index $k \in \{0, 1\}$ of the secret he is interested in, Bob computes $B' = (A_k)^b$ and sends it to Alice.
4. For each $i \in \{0, 1\}$, Alice computes $B'^{a_i^{-1}}$ where $a_i^{-1}$ is the inverse of $a_i$ modulo $\#G$, and encrypts her secret $s_i$ with the key derived from this computed value. She sends Bob the ciphertexts $S_0 = \texttt{Enc}(s_0, \texttt{KDF}(B'^{a_0^{-1}}))$ and $S_1 = \texttt{Enc}(s_1, \texttt{KDF}(B'^{a_1^{-1}}))$.
5. Bob computes $\texttt{Enc}^{-1}(S_k, \texttt{KDF}(B))$.

Correctness of the protocol follows from the identity $B'^{a_k^{-1}} = ((g^{a_k})^b)^{a_k^{-1}} = g^b = B$. As above, it can be interpreted in terms of commuting maps $\phi_{a_0}$, $\phi_{a_1}$ and $\phi_b$, see Fig. 5. If we compare to Fig. 1, we see that the direction of the lower-right arrows have been reversed, and only one of them completes a

**Alice** — **Bob**

secrets $s_0$, $s_1$ — secret $k \in \{0, 1\}$

agree on $G = \langle g \rangle$

chooses $a_0, a_1 \in_R (\mathbb{Z}/\#G\mathbb{Z})^*$ — chooses $b \in_R (\mathbb{Z}/\#G\mathbb{Z})^*$

computes $A_0 = g^{a_0}$, $A_1 = g^{a_1}$ — computes $B = g^b$

$$\xrightarrow{A_0, A_1}$$

computes $B' = (A_k)^b$

$$\xleftarrow{B'}$$

computes

$S_0 = \texttt{Enc}(s_0, \texttt{KDF}(B'^{a_0^{-1}}))$

$S_1 = \texttt{Enc}(s_1, \texttt{KDF}(B'^{a_1^{-1}}))$

$$\xrightarrow{S_0, S_1}$$

computes $\texttt{Enc}^{-1}(S_k, \texttt{KDF}(B))$

**Fig. 4.** Our DH-based oblivious transfer protocol.

$$\begin{tikzcd}
& A_0 = g^{a_0} \arrow[rdd, "\phi_b"] & \\
& A_1 = g^{a_1} & \\
g \arrow[ruu, "\phi_{a_0}"] \arrow[ru, "\phi_{a_1}"'] \arrow[rdd, "\phi_b"'] & & B' = (A_0)^b \arrow[ld, "\phi_{a_1^{-1}}"'] \arrow[ldd, "\phi_{a_0^{-1}}"] \\
& B'^{a_1^{-1}} & \\
& B = g^b = B'^{a_0^{-1}} &
\end{tikzcd}
\qquad
\begin{tikzcd}
& A_0 = g^{a_0} & \\
& A_1 = g^{a_1} \arrow[rdd, "\phi_b"] & \\
g \arrow[ruu, "\phi_{a_0}"] \arrow[ru, "\phi_{a_1}"'] \arrow[rdd, "\phi_b"'] & & \\
& & B' = (A_1)^b \arrow[ld, "\phi_{a_1^{-1}}"'] \arrow[ldd, "\phi_{a_0^{-1}}"] \\
& B = g^b = B'^{a_1^{-1}} & \\
& B'^{a_0^{-1}} &
\end{tikzcd}$$

**Fig. 5.** Another view of our DH-based OT protocol (left, $k = 0$; right, $k = 1$)

commutative diagram; the second one points to a value that Bob should not be able to compute.

As discussed above, this actually implements a *random* OT scheme: after the two first exchanges, Alice has two random (but related) elements $B'^{a_0^{-1}}$ and $B'^{a_1^{-1}}$, and only one of them is known to Bob, but at this point Alice's secrets have not yet been involved. The use of a symmetric encryption scheme together with a key derivation function gives the $\binom{2}{1}$-OT protocol.

### 2.4 Security against a malicious sender

The goal of a malicious Alice is to discover the secret bit $k \in \{0, 1\}$ of Bob. In both protocols, the only information she has access to is Bob's computed value $B' = (A_k)^b$. If Alice complies with the protocol, and the order of the group $G$ is indeed prime as specified, then $A_0$ and $A_1$, which are equal to either $(r_0)^a$ and $(r_1)^a$ or $g^{a_0}$ and $g^{a_1}$, are both generators of the group $G$. Since $b$ is uniformly distributed in $\{1, \ldots, \#G - 1\} \simeq (\mathbb{Z}/\#G\mathbb{Z})^*$, the element $B' = (A_k)^b$ is also uniformly distributed in $G \setminus \{e\}$ (where $e = g^0$ is the neutral element) and therefore leaks no information about $k$ to Alice.

A malicious Alice could, however, send Bob elements $A_0, A_1$ that are not of the specified form. But for $B' = (A_k)^b$ not to be uniformly distributed she needs $A_0$ or $A_1$ not to be a generator of $G$. As long as $G$ is of prime order, this means setting $A_0$ or $A_1$ to $e$, which Bob can detect easily. Otherwise, Alice could try working in a group $G$ of composite order. This is only possible if Bob does not check the order of the agreed-upon group $G$, or if Alice sends elements $A_0$ and $A_1$ that are not in $G$, in the spirit of the invalid curve attack [5]. In any case, as long as Bob performs some elementary checks – namely, that $G$ has indeed prime order, that $A_0$ and $A_1$ belong to $G$ and are different from $e$ – then Alice obtains no information whatsoever about Bob's secret bit $k$.

### 2.5 Security against a malicious receiver

The goal of a malicious Bob is to decrypt, or at least gain information, on both of Alice's secrets $s_0$ and $s_1$. A difficulty in the analysis is that Bob is not constrained to follow the protocol: instead of sending $B' = (A_k)^b$, he can send Alice any element of his choice in $G$. As discussed above, Alice has no mean to ensure the validity of Bob's transmitted value; doing otherwise would require expensive validation mechanisms, such as providing a zero-knowledge proof that Bob knows the logarithm of $B'$ in basis either $A_0$ or $A_1$.

The security of oblivious transfer protocols with respect to the sender's secrets is often defined in terms of an ideal functionality, but this makes for difficult proofs outside of the random oracle model. We prefer to define this security in terms of the following indistinguishability game.

**Indistinguishability game for oblivious transfer:**

Given a message length $n$ and a threshold value $\epsilon > 0$ :

- Bob sends Alice two couples of distinct messages $(m_0, m'_0)$ and $(m_1, m'_1)$ of his choice, of same length $n$;
- Alice picks randomly, uniformly and independently $s_0 \in \{m_0, m'_0\}$ and $s_1 \in \{m_1, m'_1\}$;
- Alice and Bob perform the oblivious transfer protocol with $s_0$ and $s_1$;
- Bob proposes two guesses $p_0$ and $p_1$; he wins if

$$P(p_0 = s_0 \text{ and } p_1 = s_1) - P(p_0 = s_0)\, P(p_1 = s_1) \geq \epsilon$$

or

$$\min\left(P(p_0 = s_0) - 1/2,\ P(p_1 = s_1) - 1/2\right) \geq \epsilon.$$

We say that an oblivious transfer protocol is *semantically secure* if a polynomially-limited Bob cannot win this game when $\epsilon$ is a polynomially-negligible function in the security parameter. The rationale behind this definition is that Bob should not be able to extract information about both $s_0$ and $s_1$. The first inequality implies that any useful information about the couple $(s_0, s_1)$ comes from information on $s_0$ and $s_1$ separately; the next inequality means that Bob cannot correctly guess both $s_0$ and $s_1$ with probability greater than 1/2, i.e. he cannot have useful information on $s_0$ and $s_1$ simultaneously. Overall, this definition of semantic security captures the notion that any useful information gained by Bob on one of Alice's secrets forbids him to gain any useful information on the other secret.

**Security analysis in the random oracle model.**

Obviously, the practical security of the random OT schemes we have presented depends on the underlying encryption and key derivation functions `Enc` and `KDF`, and they cannot provide a perfect secrecy as it is the case for Bob's secret $k$. Let us assume for the moment that `Enc` combined with `KDF` operates as a random oracle; in this model, Bob cannot gain any information on $s_0$ and $s_1$ if he does not know the encryption keys. For instance, as in [3,24], one can simply set $\texttt{Enc}(s, \texttt{KDF}(k)) = s \oplus H(k)$ where $H$ is a random oracle (in practice, a cryptographic hash function).

Then in order to obtain any information on both messages, Bob must be able to recover both encryption keys. In our protocol, this means being able to compute $B'^{a_0^{-1}}$ and $B'^{a_1^{-1}}$ for an element $B'$ of Bob's choice, knowing only $g$, $g^{a_0}$ and $g^{a_1}$. A trivial solution for Bob is to send Alice $B' = e$, but she can easily detect that and abort the communication in that case. Otherwise, Bob has to solve the following problem.

**2-inverse computational Diffie-Hellman problem (2-inv-CDHP):** Given a cyclic group $G = \langle g \rangle$ of prime order and elements $g^\alpha$ and $g^\beta$, produce a triple $(X, Y, Z)$ such that $X \neq e$ and $Y = X^{\alpha^{-1}}$ and $Z = X^{\beta^{-1}}$.

If Bob can solve the computational Diffie-Hellman problem (CDHP), he can easily solve 2-inv-CDHP by producing $(g^{\alpha\beta}, g^\beta, g^\alpha)$, or more generally $((g^{\alpha\beta})^x, (g^\beta)^x, (g^\alpha)^x)$ for any $x$ coprime to $\#G$. On the other hand, if for any $X \in G$, Bob can produce elements $Y, Z$ such that $Y = X^{\alpha^{-1}}$ and $Z = X^{\beta^{-1}}$, then setting $X = g$ he can solve the inverse Diffie-Hellman problem (computing $g^{\alpha^{-1}}$), which is equivalent to the standard CDHP. However, Bob only has to produce one such triple for an $X$ of his choice. Thus in theory, Bob could find any triple that is easier to compute than $(g^{\alpha\beta}, g^\beta, g^\alpha)$ or $(g, g^{\alpha^{-1}}, g^{\beta^{-1}})$. But in practice, we do not see how this additional freedom can be used and we believe this new problem to be as hard as CDHP.

Actually, it is reminiscent of the "2-out-of-3" Diffie-Hellman problem [22], which consists, given $g, g^\alpha$ and $g^\beta$, in producing a couple $(X, T)$ where $T = X^{\alpha\beta}$. Although there does not seem to be a reduction between 2-out-of-3 DHP and 2-inv-CDHP, in both cases the absence of restriction on $X$ implies that there is no obvious reduction from CDHP. Moreover, Kunz-Jacques and Pointcheval [22] have proved that the 2-out-of-3 problem is difficult in the generic group model, and their method can be adapted to our problem. We recall that in the generic group model, all details about the group $G$ are masked by a random bijective encoding $\sigma : G \to I$ and its inverse $\tau : I \to G$, where $I$ can be taken as $\{1, \ldots, \#G\}$. Any operations on the group $G$ are queried to an oracle, that on input $(a, x, a', x') \in (\mathbb{Z} \times I)^2$ answers[2] $\sigma(\tau(x)^a.\tau(x')^{a'})$. An algorithm that works in the generic group model (a generic algorithm) can therefore only rely on group operations and equality testing. In this model, we obtain the following result (see Appendix A for the proof), which implies that a generic algorithm needs $\Omega(\sqrt{\#G})$ operations in order to solve 3-inv-CDHP with a non-negligible probability.

**Theorem 1.** *The probability of solving 2-inv-CDHP after $q_G$ oracle queries is bounded by* $\frac{(3q_G+4)^2}{2\#G} + \frac{1}{\#G^2} = O(q_G^2/\#G)$.

Note finally that Bob can of course produce couples of the form $(X, X^{\alpha^{-1}})$ or $(X, X^{\beta^{-1}})$ by setting $X = (g^\alpha)^x$ or $(g^\beta)^x$, and this is exactly how he can decrypt one of Alice's ciphertexts in our protocol.

The security of Wu-Zhang-Wang protocol in the random oracle model relies on the hardness of a different problem. Indeed, to gain information on both of Alice's secrets in this protocol, Bob must compute $r_0$ and $r_1$ from the only information available to him, namely $(r_0)^a$, $(r_1)^a$, and the image $B'^{a^{-1}}$ under

[2] Other models only allow queries of the form $\sigma(\tau(x).\tau(x'))$ or $\sigma((\tau(x))^{-1})$, but this does not fundamentally alter our result.

the exponentiation by $a^{-1}$ of the element $B'$ of his choice. This is formalized in the following problem.

**One-more exponentiation problem (1MEP):**
Given a cyclic group $G = \langle g \rangle$ of prime order, two non-neutral elements $Y$ and $Z$, and a secret integer $\alpha \in \{1, \ldots, \#G - 1\}$,

- Bob submits an element $X \in G$ of his choice to an oracle, that outputs $X^\alpha$;
- then Bob must produce $Y^\alpha$ and $Z^\alpha$.

This problem is reminiscent of several non-standard Diffie-Hellman problems, most notably the "static" one-more Diffie-Hellman problem [6,21]. Clearly, Bob can solve 1MEP if he can solve the computational Diffie-Hellman problem (twice, with inputs $X$, $X^\alpha$, $Y$ and then $X$, $X^\alpha$, $Z$). On the other hand, for an honest-but-curious Bob who follows the protocol and submits either $Y$ or $Z$, solving 1MEP is equivalent to solving the CDHP with inputs $Y$, $Z$ and either $Y^\alpha$ or $Z^\alpha$. But a malicious Bob is not constrained in his choice of $X$; as in the case of 2-inv-CDHP, this freedom means that there is no trivial equivalence between 1MEP and CDHP, even though it is not at all clear how to use this freedom meaningfully. In any case, there does not seem to be any practical way to solve these problems beyond computing discrete logarithms.

**Semantic security**

However, assuming that the encryption and key derivation functions act as a random oracle is an unrealistically strong hypothesis. A more reasonable assumption is that `Enc` combined `KDF` is semantically secure [18], or more precisely satisfies the *indistinguishability under chosen-plaintext attack* (IND-CPA) property. Coming back to our indistinguishability game, under this assumption Bob cannot tell apart the encryptions of $m_0$ and $m'_0$, resp. $m_1$ and $m'_1$, with polynomially-limited resources if he does not have information on the respective encryption key.

The security of our protocol in the IND-CPA model consequently relies on the assumption that Bob cannot produce an element $B' \in G \setminus \{e\}$ such that he has information on both $B'^{a_0^{-1}}$ and $B'^{a_1^{-1}}$. This is made precise in the following decisional problem, that we present in the form of a game between Bob and an oracle.

**2-inverse decisional Diffie-Hellman problem (2-inv-DDHP):**
Given a cyclic group $G = \langle g \rangle$, elements $g^\alpha, g^\beta$, and a threshold value $\epsilon > 0$:

- Bob sends the challenge oracle an element $X \in G \setminus \{e\}$ of his choice;

– the oracle outputs two randomly ordered couples $(Y, Y')$ and $(Z, Z')$ where $Y = X^{\alpha^{-1}}$, $Z = X^{\beta^{-1}}$, and $Y', Z'$ are independently and uniformly random in $G \setminus \{e\}$;
– Bob proposes two guesses $G_\alpha$ and $G_\beta$; he wins if

$$P(G_\alpha = Y \text{ and } G_\beta = Z) - P(G_\alpha = Y)\, P(G_\beta = Z) \geq \epsilon$$

or

$$\min\left(P(G_\alpha = Y) - 1/2,\ P(G_\beta = Z) - 1/2\right) \geq \epsilon.$$

As in the oblivious transfer indistinguishability game, the first inequality signifies that any useful information on the couple $(Y, Z)$ comes from information on $Y$ and $Z$ separately, whereas the second inequality means that Bob cannot have useful information on $Y$ and $Z$ simultaneously. But Bob can of course identify either $Y$ or $Z$ by submitting $X = (g^\alpha)^x$ or $(g^\beta)^x$ for an $x$ of his choice, hence the $1/2$; if the 2-inv-DDHP is hard in $G$, he cannot do better (with polynomially-limited resources).

There is an obvious reduction from 2-inv-CDHP to 2-inv-DDHP, and also from the standard decisional Diffie-Hellman problem (DDHP). Actually, the decisional problem closest to ours is the inverse decisional Diffie-Hellman problem (inv-DDHP, see [1]): given $g, g^\alpha$ and $h$, determine if $h = g^{\alpha^{-1}}$. If Bob can solve inv-DDHP, he can solve 2-inv-DDHP by submitting $X = g$. As with the computational problem, there is no obvious reduction from 2-inv-DDHP to inv-DDHP (and neither is there a reduction from inv-DDHP to DDHP), because of the additional freedom in the choice of $X$, but we do not believe this freedom to be practically usable.

As a matter of fact, even if Bob manages to obtain some partial information on both Alice's encryption keys $B'^{a_0^{-1}}$ and $B'^{a_1^{-1}}$, he will probably not be able to use it to gain partial information on both secrets $s_0$ and $s_1$, although this claim clearly depends of the encryption scheme used (he would need some kind of related key attacks). Nevertheless, it is safer to implement our oblivious transfer protocol in a group where the decisional Diffie-Hellman problem is hard, for instance on elliptic curves that are not pairing-friendly.

For Wu-Zhang-Wang protocol, however, the IND-CPA property is not enough to guarantee the semantic security of the overall scheme. The problem is that the decisional version of the one-more exponentiation problem (1MEP) is easy: by submitting $Y/Z$ to the exponentiation oracle, Bob recovers $Y^\alpha/Z^\alpha$ and therefore gains information on the couple $(Y^\alpha, Z^\alpha)$. This is exactly the reason why the original version of Wu-Zhang-Wang protocol was insecure and had to be transformed in a random OT scheme. As remarked just above, this is an actual weakness only if Bob manages to mount a kind of related key attack. But in any case, achieving semantic security for Wu-Zhang-Wang protocol would require not only the hardness of 1MEP, but also some kind of non-standard indistinguishability property of the underlying encryption scheme.

### 2.6 Comparison between the two schemes

From a complexity point of view, we can compare the two schemes by counting the number of group exponentiations, which are usually the most expensive operations. We can see that Wu-Zhang-Wang protocol requires five exponentiations, against six for our proposal, and is thus slightly more efficient. This is however no longer true in the supersingular isogeny setting, as explained in Sect. 4.3.

Note that the protocols, as presented above, actually implement $\binom{2}{1}$ (or 1-out-of-2) oblivious transfer. Turning them into $\binom{n}{1}$-OT can be done using the classical Naor-Pinkas transform. It only requires $O(\ln(n))$ parallel executions of the first steps of the protocol, and thus only $O(\ln(n))$ exponentiations; but obviously, Alice must still send $O(n)$ encrypted messages in the final step. We refer to Naor and Pinkas original article [25] for more details. Achieving $\binom{n}{t}$-OT is a different task. Wu-Zhang-Wang protocol admits a solution with $O(n+t)$ operations, as explained in the original paper [37], whereas our protocol still necessitates $t$ executions of the $\binom{n}{1}$ scheme.

From a security point of view, we have seen that the two schemes relies on distinct hardness assumptions. Still, outside of the random oracle model Wu-Zhang-Wang protocol is weaker than ours, and cannot offer semantic security under standard indistinguishability assumptions on the underlying symmetric encryption scheme.

## 3 The De Feo-Jao-Plût supersingular isogeny key exchange

Let $E$ and $E'$ be two elliptic curves defined over the same finite field $\mathbb{F}_q$ (we refer to [32] for more details on elliptic curves and isogenies). By a theorem of Tate, we know that there exists an isogeny $\phi : E \to E'$ defined over $\mathbb{F}_q$ if and only if $E$ and $E'$ have the same number of $\mathbb{F}_q$-rational points, and this can be checked quite efficiently. On the other hand, finding such an isogeny $\phi$, or equivalently determining its kernel, is usually much more difficult.

Actually, this gives a construction of a one-way function. Starting from a subgroup $G$ of $E(\mathbb{F}_q)$, Vélu's formulae [36] allow one to compute the curve $E' \simeq E/G$ and the corresponding isogeny $\phi : E \to E'$ using $O(\#G)$ operations in $E$. But when the order of $G$ is smooth (in applications we will have $\#G = 2^n$ or $3^m$), then $\phi$ can be efficiently computed as a composition of small degree isogenies, and the cost drops to $\tilde{O}(\log(\#G))$; see [12] for more details on the optimal computation strategy. On the other hand, the inverse function, which consists of determining $G = \ker\phi$ from $E$, $E'$ and potential other information such as $\#G = \deg\phi$, is harder to compute. How much harder depends on the setting; in the case of smooth degrees (the one we are interested in), the best known quantum attacks have subexponential complexity for ordinary elliptic curves [9], but exponential complexity for supersingular elliptic curves [34].

This one-way function can be used to construct a Diffie-Hellman-type key exchange. In this context, the exponentiation maps of the Diffie-Hellman protocol are replaced by the computation of quotient curves $E/G$, and recovering $G$ from $E$ and $E/G$ is the analog of the discrete logarithm problem. The first isogeny-based key exchange proposal (by Couveignes in 1997 [11], rediscovered ten years later by Rostovtsev and Stolbunov [30,33]) used ordinary elliptic curves. After the discovery of the quantum subexponential attack of [9], this isogeny-based key exchange protocol was adapted to the supersingular setting by De Feo, Jao and Plût [12].

The difficulty is that the analogy between exponentations and taking quotients of curves is not perfect. Indeed, in the group setting, the knowledge of $a \in (\mathbb{Z}/\#G\mathbb{Z})^*$ allows one to associate an element $g^a \in G$ to any element $g \in G$; in other words, the group $(\mathbb{Z}/\#G\mathbb{Z})^*$ acts on $G$, and the Diffie-Hellman key exchange relies on the commutativity of this action (as expressed by the commutative diagram of Fig. 1). But there is no such commutative group action for supersingular elliptic curves[3]. For any subgroup $G \subset E$, one can compute the curve $E/G$ and associated isogeny $\phi : E \to E/G$ such that $\ker \phi = G$, but there is no canonical way to extend this correspondence $E \mapsto E/G$ to all supersingular curves.

The idea of the supersingular isogeny Diffie-Hellman (SIDH) key exchange of De Feo, Jao and Plût is to work with two different torsion subgroups of a supersingular curve $E$ defined over $\mathbb{F}_{p^2}$. We will assume that the full $2^n$ and $3^m$ torsion of $E$ is defined over $\mathbb{F}_{p^2}$, where $n$ and $m$ are integers related to the security level (typically $100 \leq n \leq 500$) such that $2^n \approx 3^m$. Actually, any couple of small prime numbers can be used intead of 2 and 3; in the notations of [12], we have chosen $e_A = 2$, $\ell_A = n$, $e_B = 3$ and $\ell_B = m$ to simplify the presentation. The protocol begins as follows:

- Alice and Bob, the two participants in the key exchange protocol, each choose a subgroup of $E$: Alice chooses a cyclic subgroup $G_A = \langle R_A \rangle \subset E[2^n]$ of order $2^n$, and Bob a cyclic subgroup $G_B = \langle R_B \rangle \subset E[3^m]$ of order $3^m$.
- Alice computes the curve $E_A \simeq E/\langle R_A \rangle$ with corresponding isogeny $\phi_A : E \to E_A$ and sends $E_A$ to Bob; Bob computes the curve $E_B \simeq E/\langle R_B \rangle$ with corresponding isogeny $\phi_B : E \to E_B$ and sends $E_B$ to Alice.

Now we would like Alice (resp. Bob) to compute an isogeny $\phi'_A : E_B \to E_{BA}$ (resp. $\phi'_B : E_A \to E_{AB}$) that is in some sense "parallel" to $\phi_A : E \to E_A$ (resp. to $\phi_B : E \to E_B$). Of course, we also want $E_{AB} \simeq E_{BA}$, so that Alice and Bob can use the common $j$-invariant $j(E_{AB}) = j(E_{BA})$ as a shared secret. A natural solution is to take $\ker \phi'_A = \phi_B(G_A) = \langle \phi_B(R_A) \rangle$ and $\ker \phi'_B = \phi_A(G_B) =$

[3] This commutative group action does exist, however, for ordinary elliptic curves; but this is precisely the basis of the quantum attack on the computational isogeny problem.

$\langle \phi_A(R_B)\rangle$; then

$$E_{BA} \simeq E_B/\langle \phi_B(R_A)\rangle \simeq E/\langle R_A, R_B\rangle \simeq E_A/\langle \phi_A(R_B)\rangle \simeq E_{AB}.$$

But Alice cannot ask Bob to compute $\phi_B(R_A)$: if it transits over an insecure communication channel, any eavesdropper can compute the final shared value $j(E_{AB}) = j(E_A/\langle \phi_A(R_B)\rangle)$. De Feo, Jao and Plût's solution is to fix a basis $(U, V)$ of $E[2^n]$ and a basis[4] $(P, Q)$ of $E[3^m]$ and to require Alice, resp. Bob, to transmit $\phi_A(P)$ and $\phi_A(Q)$ in addition to $E_A$, resp. $\phi_B(U)$ and $\phi_B(V)$ in addition to $E_B$. The protocol can then resume as follows:

- Alice computes $x_A, y_A \in \mathbb{Z}/2^n\mathbb{Z}$ such that $R_A = x_AU + y_AV$ (this is possible because the discrete logarithm problem is easy in $E[2^n]$). Alternatively, and preferably, she had chosen $R_A$ as $x_AU + y_AV$ by sampling $x_A$ and $y_A$ randomly in $\mathbb{Z}/2^n\mathbb{Z}$ such that at least one of them is coprime to 2.
  After receiving $E_B$, $\phi_B(U)$ and $\phi_B(V)$, she computes $\phi_B(R_A) = x_A\phi_B(U) + y_A\phi_B(V)$ and $E_{BA} \simeq E_B/\langle x_A\phi_B(U) + y_A\phi_B(V)\rangle$.
- Bob does the same and computes $E_{AB} \simeq E_A/\langle x_B\phi_A(P) + y_B\phi_A(Q)\rangle$ where $x_B, y_B \in \mathbb{Z}/3^m\mathbb{Z}$ are such that $R_B = x_BP + y_BQ$.

In practice, with a small loss of generality we can assume that $R_A = U + aV$ and $R_B = P + bQ$ where $a$, resp. $b$ are chosen randomly and uniformly from $\mathbb{Z}/2^n\mathbb{Z}$, resp. $\mathbb{Z}/3^m\mathbb{Z}$. The final protocol is summed up by the commutative diagram of Fig. 6.

$$\begin{tikzcd}
 & \begin{array}{c} E_A \simeq E/\langle U + aV\rangle, \\ \phi_A(P), \phi_A(Q) \end{array} \arrow[dr, "\phi_B'"] & \\
E, U, V, P, Q \arrow[ur, "\phi_A"] \arrow[dr, "\phi_B"'] & & \begin{array}{c} E_A/\langle \phi_A(P) + b\,\phi_A(Q)\rangle \\ \simeq E_B/\langle \phi_B(U) + a\,\phi_B(V)\rangle \end{array} \\
 & \begin{array}{c} E_B \simeq E/\langle P + b\,Q\rangle, \\ \phi_B(U), \phi_B(V) \end{array} \arrow[ur, "\phi_A'"'] &
\end{tikzcd}$$

**Fig. 6.** De Feo-Jao-Plût SIDH key exchange

The security of this scheme corresponds to the hardness of the analog of the computational Diffie-Hellman problem (CDHP):

[4] This corresponds to $(P_A, Q_A)$ and $(P_B, Q_B)$ in the notations of [12].

**Supersingular Computational Diffie-Hellman Problem** (SSCDH [12]): Let $E$ be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$ with rational $2^n$ and $3^m$ torsion, and let $(U, V)$ and $(P, Q)$ be bases of $E[2^n]$ and $E[3^m]$ respectively. Let $\phi_A : E \to E_A$ and $\phi_B : E \to E_B$ be isogenies such that $\ker \phi_A = \langle U + aV \rangle$ and $\ker \phi_B = \langle P + bQ \rangle$, where $a, b$ are chosen randomly and uniformly in $\mathbb{Z}/2^n\mathbb{Z}$ and $\mathbb{Z}/3^m\mathbb{Z}$.
Given the curves $E$, $E_A$, $E_B$ and the points $\phi_A(P), \phi_A(Q), \phi_B(U), \phi_B(V)$, find the $j$-invariant of $E/\langle U + aV, P + bQ \rangle$.

There is a similar decisional problem, the Supersingular Decisional Diffie-Hellman Problem (SSDDH); we refer to [12] for its formalization. Currently, the best approach to solve this problem is to recover $\ker \phi_A$ from the knowledge of $E$, $E_A$ and $\phi_A(P)$ and $\phi_A(Q)$; this is the SIDH analog of the computation of discrete logarithms.

**Computational Supersingular Isogeny Problem** (CSSI [12]): Let $E$ be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$ with rational $2^n$ and $3^m$ torsion, and let $(U, V)$ and $(P, Q)$ be bases of $E[2^n]$ and $E[3^m]$ respectively. Let $\phi_A : E \to E_A$ be an isogeny such that $\ker \phi_A = \langle U + aV \rangle$ where $a$ is chosen randomly and uniformly in $\mathbb{Z}/2^n\mathbb{Z}$.
Given the curves $E$, $E_A$ and the points $\phi_A(P), \phi_A(Q)$, determine $\ker \phi_A$.

Of course, we can swap the $2^n$ and $3^m$ torsion and obtain a similar statement. Compared to the one-way function described at the beginning of this section, here an attacker has access to the images of $P$ and $Q$. However, currently there is no known algorithm that exploits meaningfully of this extra information, at least when $2^n \approx 3^m$ (see however [27]), and the best known quantum attack is the claw finding method of [34], with exponential complexity.

# 4 SIDH-based oblivious transfer

## 4.1 Basic outline

**From SIDH to OT.** Our goal in this section is to construct isogeny-based, post-quantum oblivious transfer protocols, that are the analog in the SIDH setting of the group-based OT protocols presented in Sect. 2. We start with our new protocol (Sect. 2.3), which is somehow simpler to adapt; Wu-Zhang-Wang protocol will be treated in Sect. 4.3.

We follow closely the blueprint of the method presented in Sect. 2.3; the resulting construction is illustrated in Fig. 7. Instead of computing only one curve $E_A$ and the corresponding isogeny $\phi_A : E \to E_A$ as in the SIDH key exchange, Alice now computes two curves $E_{A,0} \simeq E/\langle R_0 \rangle$ and $E_{A,1} \simeq E/\langle R_1 \rangle$, and the corresponding isogenies $\phi_{A,i} : E \to E_{A,i}$ of degree $2^n$. She transmits

Bob the two curves, one for each of her secrets, together with auxiliary data (as above, the image of a fixed basis of $E[3^m]$). Then Bob computes his part, namely, the two curves $E_B \simeq E/\langle R_B \rangle$ and $E'_B \simeq E_{A,k}/\langle \phi_{A,k}(R_B) \rangle$, where $k \in \{0,1\}$ still stands for the index of the secret Bob is interested in, and the corresponding "parallel" isogenies $\phi_B : E \to E_B$ and $\phi'_B : E_{A,k} \to E'_B$

$$\begin{tikzcd}
& \begin{array}{c} E_{A,0} \simeq E/\langle R_0 \rangle, \\ \phi_{A,0}(P), \phi_{A_0}(Q) \end{array} & \\
& \begin{array}{c} E_{A,1} \simeq E/\langle R_1 \rangle, \\ \phi_{A,1}(P), \phi_{A,1}(Q) \end{array} \arrow[dr, "\phi'_B"] & \\
E, P, Q \arrow[uur, bend left, "\phi_{A,0}"] \arrow[ur, "\phi_{A,1}"] \arrow[dr, "\phi_B"'] & & E'_B \simeq E_{A,k}/\langle \phi_{A,k}(P) + b\,\phi_{A,k}(Q) \rangle \arrow[dl, dotted, "??"] \\
& E_B \simeq E/\langle P + bQ \rangle &
\end{tikzcd}$$

**Fig. 7.** First steps of the SIDH-based oblivious transfer (case $k = 1$)

In the key exchange protocol, Bob transmitted Alice the curve $E_B$ together with the image by $\phi_B$ of a fixed basis of $E[2^n]$; this allowed Alice to compute the isogeny $\phi'_A$ "parallel" to $\phi_A$, whose kernel is $\langle \phi_B(R_A) \rangle$. But for the oblivious transfer protocol, we want to proceed the other way round: Bob sends Alice the curve $E'_B$, which is $3^m$-isogenous to $E_{A,0}$ or $E_{A,1}$, but Alice does not know to which one. Similarily to Sect. 2.3, the key point is thus to "reverse" the map $\phi'_{A,k}$ going from $E_B$ to $E'_B$. In the isogeny setting, what we are interested in are actually the domain and codomain of the map $\phi'_{A,k}$, and our goal becomes to compute the dual isogeny $\widehat{\phi}'_{A,k} : E'_B \to E_B$.

**Dual isogenies.** It is a standard fact about elliptic curves, see for instance [32], that for any isogeny $\phi : E \to E'$ between two elliptic curves there exists another isogeny

$$\widehat{\phi} : E' \to E,$$

called the dual isogeny of $\phi$, such that $\widehat{\phi} \circ \phi$ (resp. $\phi \circ \widehat{\phi}$) is the multiplication-by-$\deg \phi$ endomorphism of $E$ (resp. of $E'$). It also satisfies $\deg \widehat{\phi} = \deg \phi$, $\widehat{\widehat{\phi}} = \phi$, and $\widehat{\phi}$ has the same field of definition as $\phi$.

If $\phi : E \to E'$ is an isogeny of degree $d$ coprime to the characteristic, given by a cyclic kernel $\ker \phi = \langle R \rangle \subset E[d]$, then the kernel of $\widehat{\phi}$ can be easily described.

Indeed, let $T \in E$ be such that $E[d] = \langle R, T\rangle$. Since $\ker(\widehat{\phi} \circ \phi) = E[d] = \langle R, T\rangle$ and $\phi$ is surjective, it follows that $\ker \widehat{\phi} = \phi(E[d]) = \langle \phi(R), \phi(T)\rangle = \langle \phi(T)\rangle$. When all the $d$-torsion is rational, it is not difficult to find such a complementary generator $T$ of $E[d]$, after which $\phi(T)$ and $\widehat{\phi}$ can be computed using Vélu's formulae.

**Completing the oblivious transfer.** In order to complete the protocol, Alice will compute two isogenies: one which will be parallel to $\hat{\phi}_{A,k}$, and the other a bogus one, arriving at some unknown curve. As in De Feo-Jao-Plût construction, Alice needs extra information to compute efficiently these maps. What she can do easily is find a generator of the kernel of the dual isogeny $\widehat{\phi}_{A,i} : E_{A,i} \to E_A$ (for each $i \in \{0, 1\}$), by taking the image by $\phi_{A,i}$ of a generator $T_i$ of a complement of $\ker \phi_{A,i}$ in $E[2^n]$. Now she can compute $\widehat{\phi}'_{A,k}$, even without knowing $k$, if she has access to $\phi'_B(\phi_{A,k}(T_k))$. But she cannot give Bob $\phi_{A,i}(T_i)$: this discloses $\ker \widehat{\phi}_{A,i}$, from which Bob or any eavesdropper can recover $\ker \phi_{A,i}$, ruining the protocol. One way to achieve that while preventing Bob from gaining useful information is to ask him to compute and send Alice the image by $\phi'_B$ of a basis of $E_{A,k}[2^n]$; we will see however in Sect. 5.1 that some care must be taken in doing so.

More precisely, a basis $(U_0, V_0)$ of $E_{A,0}[2^n]$ is chosen, as well as a basis $(U_1, V_1)$ of $E_{A,1}[2^n]$, and Bob transmits $\phi'_B(U_k)$ and $\phi'_B(V_k)$ to Alice together with $E'_B$. Then Alice writes $\phi_{A,0}(T_0)$ and $\phi_{A,1}(T_1)$ as $x_0U_0 + y_0V_0$ and $x_1U_1 + y_1V_1$, and she computes the two curves $F_0 \simeq E'_B/\langle x_0\phi'_B(U_k) + y_0\phi'_B(V_k)\rangle$ and $F_1 \simeq E'_B/\langle x_1\phi'_B(U_k) + y_1\phi'_B(V_k)\rangle$. One of these two curves, $F_k$, corresponds to the quotient $E'_B/\langle \phi'_B(T_k)\rangle$, which is isomorphic to the curve $E_B$ computed by Bob; the other one is random. Thus Alice has obtained two values $j(F_0)$ and $j(F_1)$, such that one of them, $j(F_k) = j(E_B)$, is known to Bob, but Alice does not know which one. They can be used as key seeds to encrypt Alice's secrets using a key derivation function and a symmetric cipher, as in the group-based setting. The complete construction is illustrated in Fig. 8 below.

### 4.2 A first protocol

We now detail the protocol sketched above for the $\binom{2}{1}$-oblivious transfer; as in Sect. 2.6, it can be easily turned into a $\binom{n}{1}$-OT. Alice has two secrets $s_0, s_1$ and Bob wants to learn one of them, without allowing Alice to know which one; and Alice does not want Bob to learn both secrets. Let $k \in \{0, 1\}$ be the index of Bob's choice.

1. Setup: Alice and Bob agree on security parameters $n, m$ such that $2^n \approx 3^m$, a supersingular curve $E$ defined over a finite field $\mathbb{F}_{p^2}$ such that $E[2^n3^m] \subset E(\mathbb{F}_{p^2})$, and points $P, Q$ generating $E[3^m]$. They also agree on a secure symmetric encryption protocol `Enc` such as AES, and a key derivation function `KDF`.
2. - Alice chooses two different cyclic random subgroups $G_0 = \langle R_0\rangle, G_1 = \langle R_1\rangle$ of $E$ of order $2^n$. She also finds $T_0, T_1 \in E[2^n]$ such that $E[2^n] = \langle R_0, T_0\rangle = \langle R_1, T_1\rangle$.

$$\begin{tikzcd}
 & \begin{array}{c} E_{A,0} \simeq E/\langle R_0 \rangle, \\ \phi_{A,0}(P), \phi_{A_0}(Q), U_0, V_0 \end{array} & \\
 & \begin{array}{c} E_{A,1} \simeq E/\langle R_1 \rangle, \\ \phi_{A,1}(P), \phi_{A,1}(Q), U_1, V_1 \end{array} \arrow[dr, "\phi'_B"] & \\
E, P, Q \arrow[uur, bend left, "\phi_{A,0}"] \arrow[ur, "\phi_{A,1}"] \arrow[dr, "\phi_B"'] & & \begin{array}{c} E'_B \simeq E_{A,1}/\langle \phi_{A,1}(P) + b\,\phi_{A,1}(Q) \rangle \\ \phi'_B(U_1), \phi'_B(V_1) \end{array} \arrow[dl, "\widehat{\phi}_{A,1}"] \arrow[ddl, bend left] \\
 & \begin{array}{c} E_B \simeq E/\langle P + bQ \rangle \simeq \\ E'_B/\langle x_1 \phi'_B(U_1) + y_1 \phi'_B(V_1) \rangle \end{array} & \\
 & F_0 \simeq E'_B/\langle x_0 \phi'_B(U_1) + y_0 \phi'_B(V_1) \rangle &
\end{tikzcd}$$

**Fig. 8.** SIDH-based oblivious transfer, case $k = 1$

- For each $i \in \{0, 1\}$, she computes with Vélu's formula the curve $E_{A,i} \simeq E/G_i$ and the corresponding isogeny $\phi_{A,i} : E \to E_{A,i}$. She sends Bob $E_{A,i}, \phi_{A,i}(P), \phi_{A,i}(Q)$.

3. Bob chooses a uniformly random $b \in \mathbb{Z}/3^m\mathbb{Z}$.

   - He computes the curve $E_B \simeq E/\langle P + bQ \rangle$ and its $j$-invariant $j_B$.
   - He chooses random generators $U_0, V_0$ of $E_{A,0}[2^n]$, resp. random generators $U_1, V_1$ of $E_{A,1}[2^n]$, such that the Weil pairings $w(U_0, V_0)$ and $w(U_1, V_1)$ are equal.
   - He computes the curve $E'_B \simeq E_{A,k}/\langle \phi_{A,k}(P) + b\,\phi_{A,k}(Q) \rangle$ and the corresponding isogeny $\phi'_B : E_{A,k} \to E'_B$. He sends Alice $U_0$, $V_0$, $U_1$, $V_1$, $E'_B$, $\phi'_B(U_k)$, $\phi'_B(V_k)$.

4. For each $i \in \{0, 1\}$, Alice computes $x_i, y_i \in \mathbb{Z}/2^n\mathbb{Z}$ such that $\phi_{A,i}(T_i) = x_i U_i + y_i V_i$. She then computes $F_i \simeq E'_B/\langle x_i \phi'_B(U_k) + y_i \phi'_B(V_k) \rangle$. She computes $S_i = \texttt{Enc}(s_i, \texttt{KDF}(j(F_i)))$, the encryption of the secret $s_i$ with the key derived from the $j$-invariant of $F_i$.
   She sends Bob $S_0, S_1$.
5. Bob computes $\texttt{Enc}^{-1}(S_b, \texttt{KDF}(j_B))$.

**Alice**
secrets $s_0, s_1$

**Bob**
secret $k \in \{0,1\}$

agree on $E, P, Q$

Alice: chooses $R_0, R_1, T_0, T_1 \in_R E[2^n]$ such that $\langle R_0, T_0 \rangle = \langle R_1, T_1 \rangle = E[2^n]$

Bob: chooses $b \in \mathbb{Z}/3^m\mathbb{Z}$

Alice: for each $i \in \{0,1\}$:
computes $\phi_{A,i} : E \to E_{A,i} \simeq E/\langle R_i \rangle$

Bob: computes $E_B \simeq E/\langle P + bQ \rangle$

$$\xrightarrow[E_{A,1}, \phi_{A,1}(P), \phi_{A,1}(Q)]{E_{A,0}, \phi_{A,0}(P), \phi_{A,0}(Q)}$$

Bob:
- finds random bases $U_0, V_0$ of $E_{A,0}[2^n]$, and $U_1, V_1$ of $E_{A,1}[2^n]$ s.t. $w(U_0, V_0) = w(U_1, V_1)$
- computes $\phi'_B : E_{A,k} \to E'_B$ where $E'_B \simeq E_{A,k}/\langle \phi_{A,k}(P) + b\,\phi_{A,k}(Q) \rangle$

$$\xleftarrow{U_0, V_0, U_1, V_1, E'_B, \phi'_B(U_k), \phi'_B(V_k)}$$

Alice: for each $i \in \{0,1\}$:
- computes coordinates $(x_i, y_i)$ of $\phi_{A,i}(T_i)$ in basis $(U_i, V_i)$
- computes $F_i = E'_B/\langle x_i \phi'_B(U_k) + y_i \phi'_B(V_k) \rangle$
- computes $S_i = \mathtt{Enc}(s_i, \mathtt{KDF}(j(F_i)))$

$$\xrightarrow{S_0, S_1}$$

Bob: computes $\mathtt{Enc}^{-1}(S_k, \mathtt{KDF}(j(E_B)))$

**Fig. 9.** Our SIDH-based oblivious transfer protocol.

The correctness of the algorithm follows from the identities

$$\begin{aligned} F_k &\simeq \big((E/\langle R_k \rangle)/\langle \phi_{A,k}(P) + b\,\phi_{A,k}(Q) \rangle\big)/\langle x_k \phi'_B(U_k) + y_k \phi'_B(V_k) \rangle \\ &\simeq \big((E/\langle R_k \rangle)/\langle \phi_{A,k}(P + bQ) \rangle\big)/\langle \phi'_B(x_k U_k + y_k V_k) \rangle \\ &\simeq \big((E/\langle R_k \rangle)/\langle \phi_{A,k}(P + bQ) \rangle\big)/\langle \phi'_B(\phi_{A,k}(T_k)) \rangle \\ &\simeq (E/\langle R_k, T_k \rangle)/\langle P + bQ \rangle \\ &\simeq (E/E[2^n])/\langle P + bQ \rangle \simeq E/\langle P + bQ \rangle \simeq E_B. \end{aligned}$$

The associated diagram is presented in Fig. 8 above. Conceptually, it is the analog of Fig. 5 (except that for brevity only the case $k = 1$ is pictured), with supersingular curves and isogenies instead of group elements and exponentiation maps. When compared to Fig. 6, the lower-right isogenies have been replaced by their duals, and only one of them completes the diagram; as in the Diffie-

Hellman setting, the second one points to a curve that Bob should not be able to compute.

### 4.3 The supersingular isogeny version of Wu-Zhang-Wang protocol

The exponentiation-only OT scheme of Wu-Zhang-Wang can also be modified to work in the supersingular isogeny setting. But this translation raises some very interesting points about isogeny-based crypto. We recall that in the original Wu-Zhang-Wang protocol (Sect. 2.2), Alice's secrets $s_0$ and $s_1$ are elements of the group $G$, whereas in the random-OT version, Alice chooses random elements $r_0, r_1 \in G$. Thus for its SIDH adaptation, we need to be able to answer one of the following problems.

- **Problem 1:** is is possible to efficiently encode messages as (isomorphism classes of) supersingular elliptic curves over a given finite field?
- **Problem 2:** is it possible to efficiently sample random (isomorphism classes of) supersingular elliptic curves over a given finite field?

Both questions are not new, but satisfying answers would greatly improve the state-of-the-art in isogeny-based cryptography. Note that it is possible to efficiently construct supersingular elliptic curves over a finite field (see [8]), but the resulting curves are always quite special (usually $j = 0$ or 1728).

The difficulty with both problems is that supersingular elliptic curves form a very small proportion of all elliptic curves: over $\mathbb{F}_{p^2}$, approximately only one curve out of $p$ is supersingular. Even though testing for supersingularity can be done efficiently, this small proportion means that the strategy of sampling random curves until a supersingular one is found is prohibitively expensive. Now, a standard solution to the second problem is to run a random isogeny walk, starting from a known supersingular curve. Because of the good mixing properties of the supersingular isogeny graph, only $O(\ln(p))$ steps are needed to reach an almost uniform distribution. But even if the reached curve is random, the entity running the isogeny walk always knows the path connecting it to the starting curve; this may be a problem in some applications.

The first problem is much more difficult and has currently no solution, even partial. Isogeny walks allow to map messages to supersingular curves, but this only yields one-way functions. For this reason, we just give below the SIDH translation of the random-OT version of Wu-Zhang-Wang protocol.

1. Setup: Alice and Bob agree on security parameters $n, m$ such that $2^n \approx 3^m$, and a finite field $\mathbb{F}_{p^2}$ such that $2^n 3^m | p \pm 1$.
2. - Alice chooses two random supersingular elliptic curves $E_0$ and $E_1$ defined over $\mathbb{F}_{p^2}$ with cardinality divisible by $2^{2n} 3^{2m}$. For each $i \in \{0, 1\}$, she chooses a random subgroup $\langle R_i \rangle \subset E_i[2^n]$ of order $2^n$, as well as $T_i$ such that $\langle R_i, T_i \rangle = E_i[2^n]$, and she computes with Vélu's formulae the curve $E_{A,i} \simeq E_i / \langle R_i \rangle$ and the corresponding isogeny $\phi_{A,i} : E \to E_{A,i}$.

- Alice finds points $W_0 \in E_{A,0}$ and $W_1 \in E_{A,1}$ such that $(\phi_{A,0}(T_0), W_0)$ and $(\phi_{A,1}(T_1), W_1)$ are bases of $E_{A,0}[2^n]$ and $E_{A,1}[2^n]$ respectively, with equal Weil pairing. Using one random invertible matrix in $GL_2(\mathbb{Z}/2^n\mathbb{Z})$, she computes new bases $(U_0, V_0)$ and $(U_1, V_1)$ of $E_{A,0}[2^n]$ and $E_{A,1}[2^n]$ respectively, with equal Weil pairing, and such that $\phi(T_0) = U_0 + aV_0$ and $\phi(T_1) = U_1 + aV_1$ for a given $a \in \mathbb{Z}/2^n\mathbb{Z}$. She keeps $a$ secret and sends Bob $E_{A,i}, U_i, V_i$ for $i = 0, 1$.

3. - According to the index $k$ of the secret he is interested in, Bob chooses a random order $3^m$ subgroup $\langle P \rangle \subset E_{A,k}[3^m]$, as well as $Q$ such that $\langle P, Q \rangle = E_{A,k}[3^m]$. He computes the curve $E'_B \simeq E_{A,k}/\langle P \rangle$ and the corresponding isogeny $\phi'_B : E_{A,k} \to E_{AB}$.
   - Bob chooses a random basis $(P', Q')$ of $E'_B[3^m]$ and computes the coordinates $x, y$ of $\phi'_B(Q)$ in this basis. He sends Alice $E'_B$, $\phi'_B(U_k)$, $\phi'_B(V_k)$, $P'$, $Q'$.
4. Alice computes $E_B \simeq E'_B/\langle \phi'_B(U_k) + a\, \phi'_B(V_k) \rangle$ and the corresponding isogeny $\hat{\phi}'_{A,k} : E'_B \to E_B$. She sends Bob $E'_B$, $\hat{\phi}'_{A,k}(P')$, $\hat{\phi}'_{A,k}(Q')$.
5. For each $i \in \{0, 1\}$, Alice computes $S_i = \mathtt{Enc}(s_i, \mathtt{KDF}(j(E_i)))$, the encryption of the secret $s_i$ with the key derived from the $j$-invariant of $E_i$.
   She sends Bob $S_0, S_1$.
6. Bob computes $E'_k \simeq E_B/\langle x\, \hat{\phi}'_{A,k}(P') + y\, \hat{\phi}'_{A,k}(Q') \rangle$ and $\mathtt{Enc}^{-1}(S_k, \mathtt{KDF}(j(E'_k)))$.

$$\begin{tikzcd}
 & \begin{array}{c} E_{A,0} \simeq E_0/\langle R_0 \rangle, \\ U_0, V_0 \end{array} & & \\
 & & \begin{array}{c} E_{A,1} \simeq E_1/\langle R_1 \rangle, \\ U_1, V_1 \end{array} \arrow[ddr, "\phi'_B"] & \\
E_0 \arrow[uur, "\phi_{A,0}"] & & & \\
 & \begin{array}{c} E_1 \\ \simeq E_B/\langle x\, \hat{\phi}'_{A,k}(P') + y\, \hat{\phi}'_{A,k}(Q') \rangle \end{array} \arrow[uur, "\phi_{A,1}"] & & \begin{array}{c} E'_B \simeq E_{A,k}/\langle P \rangle, \\ \phi'_B(U_k), \phi'_B(V_k), P', Q' \end{array} \arrow[dl, "\hat{\phi}'_{A,k}"] \\
 & & \begin{array}{c} E_B \simeq E'_B/\langle \phi'_B(U_k) + a\, \phi' B(V_k) \rangle, \\ \hat{\phi}'_{A,k}(P'), \hat{\phi}'_{A,k}(Q') \end{array} \arrow[ul, "\hat{\phi}_B"] &
\end{tikzcd}$$

**Fig. 10.** SIDH version of Wu-Zhang-Wang protocol, case $k = 1$

Correctness of the protocol follows from the identities

$$\begin{aligned} E'_k &\simeq E_B/\langle \hat{\phi}'_{A,k}(\phi'_B(Q))\rangle \simeq E'_B/\langle \phi'_B(T_k), \phi'_B(Q)\rangle \\ &\simeq E_{A,k}/\langle P, T_k, Q\rangle \simeq (E_{A,k}/E_{A,k}[3^m])/\langle T_k\rangle \simeq E_{A,k}/\langle T_k\rangle \simeq E_k. \end{aligned}$$

Compared to the DH-based protocol (Fig. 2), we see in Fig. 10 that the exponentiations by $a$ and $b$ have been replaced by isogeny computations, and their inverses by taking dual isogenies. As in the De Feo-Jao-Plût protocol and our previous proposition, we need information on images of basis points to ensure commutativity. A difficulty comes from the fact that Alice must compute $\hat{\phi}'_{A,k}$, the dual to the isogeny parallel to $\phi_{A,k}$, without knowing $k$. For this reason, we need that $\phi_{A,0}(T_0)$ and $\phi_{A,1}(T_1)$, which generate the kernels of the duals $\hat{\phi}_{A,0}$ and $\hat{\phi}_{A,1}$, have the same coordinates in bases $(U_0, V_0)$ and $(U_1, V_1)$ respectively. This, and the considerations of Sect. 5.1, explain the somewhat complicated second item of step 2.

The most expensive operation in isogeny-based crypto is by far the computation of large degree isogenies. At first glance, it seems that the above protocol requires only five such operations. However as explained above, choosing the random supersingular curves $E_0$ and $E_1$ requires the computations of two additional large degree isogenies, for a total of seven operations. This is slightly more than with our first protocol, which only requires six isogeny computations.

## 5 Security analysis

### 5.1 Malicious Alice

Contrarily to the group-based setting, our SIDH-based protocols do not provide perfect secrecy for Bob's secret bit $k$. In both protocols, Alice has access to Bob's answer $E'_B$, $\phi'_B(U_k)$, $\phi'_B(V_k)$, and she knows that $E'_B$ is $3^m$-isogenous to one of the two curves $E_{A,0}$, $E_{A,1}$; recovering Bob's secret bit $k$ amounts to finding to which curve $E'_B$ is isogenous. This is the Decisional Supersingular Isogeny (DSSI) problem of De Feo-Jao-Plût [12]: given two supersingular elliptic curves defined over $\mathbb{F}_{p^2}$, determine if they are $3^m$-isogenous. A simple cardinality argument shows that it is very unlikely that $E'_B$ is $3^m$-isogenous to both $E_{A,0}$ and $E_{A,1}$ (there are about $p/12$ supersingular curves defined over $\mathbb{F}_{p^2}$, while the number of $3^m$-isogenies from $E'_B$ is of the order of $3^m \leq \sqrt{p}$). So a brute-force approach can, in theory, succeed in finding $k$; nevertheless this problem is expected to be computationally intractable.

However Alice has more information than just $E'_B$: she knows $\phi'_B(U_k)$ and $\phi'_B(V_k)$, the images by Bob's isogeny of the basis points $U_k, V_k$. In particular, she can compute the Weil pairings of $\phi'_B(U_k)$ with $\phi'_B(V_k)$, $U_0$ with $V_0$, and $U_1$ with $V_1$. Because of the property of the Weil pairing, it holds that

$$w(\phi'_B(U_k), \phi'_B(V_k)) = w(U_k, V_k)^{\deg \phi'_B} = w(U_k, V_k)^{3^m}.$$

Thus if $w(U_0, V_0) \neq w(U_1, V_1)$, Alice can find which one is equal to $w(\phi'_B(U_k), \phi'_B(V_k))$ when put to the $3^m$-th power, and determine Bob's secret $k$.

For this reason, such values of $U_0, V_0$ and $U_1, V_1$ have been avoided in our protocols (one cannot simply choose $w(U_i, V_i) = 1$ since in that case $(U_i, V_i)$ do not form a basis of $E_{A,i}[2^n]$). In the first protocol of Sect. 4.2, we tasked Bob with the responsability of choosing $U_i, V_i$, see second item of step 3. It is not possible do that in the second protocol of Sect. 4.3, because the points $\phi_{A,0}(T_0)$ and $\phi_{A,1}(T_1)$, which are known only to Alice, must have the same coordinates in bases $(U_0, V_0)$ and $(U_1, V_1)$ respectively. Consequently, Bob must imperatively check that the points sent by Alice have the same Weil pairing, and are indeed bases of $E_{A,0}[2^n]$, resp. $E_{A,1}[2^n]$.

With this extra condition, we see that our protocol requires the following extension of the DSSI problem to be computationally hard:

**Extended decisional supersingular isogeny problem (XDSSI):** Given two supersingular elliptic curves $E$ and $E'$ defined over $\mathbb{F}_{p^2}$, together with points $U, V$, $U', V'$ such that $\langle U, V \rangle = E[2^n]$, $\langle U', V' \rangle = E'[2^n]$, and $w(U, V)^{3^m} = w(U', V')$, determine if there exists an isogeny $\phi : E \to E'$ of degree $3^m$ such that $\phi(U) = U'$ and $\phi(V) = V'$.

In the SIDH context, this problem is, in fact, more natural than DSSI. It has no direct counterpart in our analogy with the standard Diffie-Hellman protocol: the only meaningful decisional version of the discrete logarithm problem is to ask, given $g \in G$, $h \in \langle g \rangle$ and a subinterval $I$ of $\{1, \ldots, \#G\}$, if $\log_{[g]}(h)$ belongs to $I$, but its difficulty is not directly relevant to the security analysis.

Currently, there is no reason to believe that XDSSI should be much weaker than its computational version. But if it were to be the case, that is, if it were computationally easy to determine whether $E$ and $E'$ are $3^m$-isogenous while the problem of determining the isogeny or its kernel remains hard, then we would have an analog of gap Diffie-Hellman groups. In particular, this would allow the construction of isogeny-based short signature schemes, à la Boneh-Lynn-Sacham [7]. We refer to Appendix B for more details.

As a final note, the above analysis actually holds for an honest-but-curious Alice. Conceivably, a malicious Alice could transmit Bob a pair of supersingular elliptic curves and basis points of her choice, that could help her discover Bob's secret. More precisely, she could send any pair of curves, although Bob can easily check that the curves he receives are indeed supersingular, and that (in our first protocol) the accompanying points form a basis of the $3^m$-torsion satisfying $w(\phi_{A,i}(P), \phi_{A,i}(Q)) = w(P, Q)^{2^n}$. However, it is expected that the (extended) decisional supersingular isogeny problem is hard for any starting curve $E$, and thus a malicious Alice has no advantage over an honest-but-curious one.

### 5.2 Malicious Bob

Most of what has been said in Sect. 2.5 about the security of the oblivious transfer schemes in the group-based setting can be transposed to the supersingular isogeny setting; in particular, we can differentiate between the random oracle model and the IND-CPA property. The difference is in the formulation of the security assumptions – besides the obvious fact that they have been much less studied than their group counterpart.

More precisely, in the random oracle model the security of our first protocol relies on the hardness of the following problem:

**2-inverse computational supersingular isogeny problem (2-inv-CSSIP):**

Let $E, E_0, E_1$ be three supersingular elliptic curves defined over $\mathbb{F}_{p^2}$ such that $E_0$ and $E_1$ are $2^n$-isogenous to $E$, and $\phi_0 : E \to E_0$, $\phi_1 : E \to E_1$ be the corresponding isogenies. Let $(P, Q)$ be a basis of $E[3^m]$ and for each $i = 0, 1$, let $(U_i, V_i)$ be a basis of $E_i[2^n]$ and $(x_i, y_i)$ be the coordinates in this basis of a generator of the dual isogeny $\widehat{\phi_i}$.

Given $E, E_0, E_1$ and the points $P, Q, U_0, V_0, U_1, V_1, \phi_0(P), \phi_0(Q), \phi_1(P), \phi_1(Q)$, find three supersingular elliptic curves $E', F_0, F_1$ and a basis $(U', V')$ of $E'[2^n]$ such that $F_0 \simeq E'/\langle x_0U' + y_0V'\rangle$ and $F_1 \simeq E'/\langle x_1U' + y_1V'\rangle$.

If one can solve the Computational Supersingular Isogeny Problem (CSSI, see Sect. 3), i.e. generators of $\ker \phi_0$ and $\ker \phi_1$ can be efficiently computed, then it is easy to obtain values for $x_0, y_0, x_1, y_1$ and solve the above problem. However, in contrast with 2-inv-CDHP, there is no obvious reduction to the SSCDH problem (Sect. 3); this is because $E, E_0, E_1$ and the associated points do not form a SIDH triple (this would need one of $E_0$ and $E_1$ to be $3^m$-isogenous to $E$ instead of $2^n$-isogenous).

Actually, it seems difficult to solve 2-inv-CSSIP without computing $x_0, y_0, x_1, y_1$, that is, solving the CSSI problem. It would require to find a curve $E'$ and points $U', V'$ such that $U'$, resp. $V'$, is related to both $U_0$ and $U_1$, resp. $V_0$ and $V_1$. This is possible for either $U_0$ and $V_0$ or $U_1$ and $V_1$, and it is precisely how the oblivious transfer protocol works, but we expect this to be computationally infeasible for both, even on a quantum computer. The only other way is to cheat and submit points $U', V'$ that do not form a basis of $E'[2^n]$, thus limiting the possible values of $x_iU' + y_iV'$. In our protocol, Alice can easily detect if Bob does that and abort the communication if necessary; in any case she should always perform this safety check (in step 4) before going any further.

If we only assume that the encryption scheme `Enc` combined with `KDF` is IND-CPA, then the decisional version of 2-inv-CSSIP must be computationally hard.

**2-inverse decisional supersingular isogeny problem (2-inv-DSSIP):** With the notations of 2-inv-CSSIP, given $E, E_0, E_1$, the points $P, Q$, $U_0, V_0$, $U_1, V_1$, $\phi_0(P), \phi_0(Q)$, $\phi_1(P), \phi_1(Q)$, and a threshold value $\epsilon > 0$:

- Bob sends the challenge oracle a supersingular elliptic curve $E'$ and a basis $(U', V')$ of $E'[2^n]$;
- the oracle outputs two randomly ordered couples $(F_0, F_0')$, $(F_1, F_1')$ of supersingular curves such that $F_0 \simeq E'/\langle x_0 U' + y_0 V'\rangle$, $F_1 \simeq E'/\langle x_1 U' + y_1 V'\rangle$, $F_0' \simeq E'/\langle W_0\rangle$ and $F_1' \simeq E'/\langle W_1\rangle$ where $W_0$ and $W_1$ are uniformly random points of $E'$ of order $2^n$;
- Bob proposes two guesses $C_0$ and $C_1$; he wins if

$$P(C_0 = F_0 \text{ and } C_1 = F_1) - P(C_0 = F_0)\, P(C_1 = F_1) \geq \epsilon$$

or

$$\min\left(P(C_0 = F_0) - 1/2,\ P(C_1 = F_1) - 1/2\right) \geq \epsilon.$$

This problem is of course easier than its computational version. But apart from that, there is no visible reduction to the SSDDH problem, nor even to the DSSI problem, and we expect it to be as difficult as 2-inv-CSSIP.

Looking now at the supersingular isogeny version of Wu-Zhang-Wang protocol, we can see that its security relies on the hardness of the analog of the one-more exponentiation problem.

**One-more isogeny computational problem (1MICP)**

Let $E_0$ and $E_1$ be two supersingular elliptic curves defined over $\mathbb{F}_{p^2}$. Let $(U_0, V_0)$, resp. $(U_1, V_1)$, be a basis of $E_0[2^n]$, resp. $E_1[2^n]$. Finally, let $a$ be a random element of $\mathbb{Z}/2^n\mathbb{Z}$.

- Bob submits a supersingular elliptic curve of his choice $E'$, together with a basis $(U', V')$ of $E'[2^n]$ and a basis $(P', Q')$ of $E'[3^m]$ to an oracle;
- the oracle outputs $E'' \simeq E'/\langle U' + aV'\rangle$, as well as the points $\phi'(P'), \phi'(Q')$, where $\phi'$ is the isogeny $E' \to E''$;
- then Bob must produce $E_0/\langle U_0 + aV_0\rangle$ and $E_1/\langle U_1 + aV_1\rangle$.

As with 2-inv-CSSIP, there is a clear reduction from this problem to the CSSI problem, but no obvious reduction to the SSCDH problem. Interestingly, in this supersingular isogeny setting, the decisional version of this problem is not easy as in the group setting (we do not give its full definition, but it follows the same distinguishability game as 2-inv-DSSIP). Indeed, because of the lack of a group law, it is difficult for Bob to submit an elliptic curve $E'$ that is related to both

$E_0$ and $E_1$. Actually, if Bob can find such a curve $E'$ isogenous both to $E_0$ and $E_1$, then he can find an isogeny between $E_0$ and $E_1$; but this is supposed to be a quantum-hard problem. Consequently, and under reasonable hardness assumptions, the supersingular isogeny version of Wu-Zhang-Wang protocol can offer a semantically secure oblivious transfer if coupled with an IND-CPA encryption scheme; this was not the case for the group-based protocol.

## 6 Conclusion

We have studied in this article two Diffie-Hellman based oblivious transfer protocols: a rewriting of the 2003 scheme of Wu, Zhang and Wang, and an entirely new one. Besides their simplicity, their main advantages are that they can be instantiated on fast Kummer surfaces, and that they give rise to post-quantum, supersingular isogeny based protocols. To the best of our knowledge, these are the only existing OT protocols with these features.

Our analysis introduces several non-standard versions of the (SI)DH problem, for which security reductions proved elusive. Nevertheless, we believe these problems to be intractable in general, and have given evidences in that direction; but obviously, further investigation by the cryptographic community is needed. As a side remark, we have shown that a hypothetical weakness of the (extended) decisional supersingular isogeny problem would ruin our SIDH OT protocols but would allow interesting isogeny-based short signature schemes.

As importantly, we hope to have demonstrated the importance of being exponentiation-only for discrete-log based schemes. Finding such a simple DLP-based signature protocol is an open problem; this would provide a practical signature protocol for isogeny-based cryptography, which is currently lacking.

## Acknowledgments

This work has been supported in part by the European Union's H2020 Programme under grant agreement number ERC-669891. The author would like to thank Luca de Feo, Charles Bouillaguet, Damien Vergnaud and Antoine Joux for their helpful discussions, and anonymous referees for their relevant remarks and for pointing us the article of Wu, Zhang and Wang.

## References

1. F. Bao, R. H. Deng, and H. Zhu. Variations of Diffie-Hellman problem. In *Information and communications security—ICICS 2003*, volume 2836 of *Lecture Note in Comput. Sci.*, pages 301–312. Springer, 2003.
2. D. Beaver. Precomputing oblivious transfer. In *Advances in Cryptology — CRYPTO 95*, volume 963 of *Lecture Note in Comput. Sci.*, pages 97–109, Berlin, Heidelberg, 1995. Springer Berlin Heidelberg.

3. M. Bellare and S. Micali. Non-interactive oblivious transfer and applications. In *Advances in Cryptology—CRYPTO 89*, volume 435 of *Lecture Notes in Comput. Sci.*, pages 547–557, 1990.
4. D. J. Bernstein, C. Chuengsatiansup, T. Lange, and P. Schwabe. Kummer strikes back: new DH speed records. In *Advances in cryptology – ASIACRYPT 2014*, volume 8873 of *Lecture Notes in Comput. Sci.*, pages 317–337. Berlin: Springer, 2014.
5. I. Biehl, B. Meyer, and V. Müller. Differential fault attacks on elliptic curve cryptosystems. (Extended abstract). In *Advances in cryptology—CRYPTO 2000*, volume 1880 of *Lecture Notes in Comput. Sci.*, pages 131–146. Berlin: Springer, 2000.
6. A. Boldyreva. Threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group signature scheme. In *Public Key Cryptography — PKC 2003*, volume 2567 of *Lecture Notes in Comput. Sci.*, pages 31–46, Berlin, Heidelberg, 2003. Springer.
7. D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. In *Advances in cryptology—ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Comput. Sci.*, pages 514–532. Springer, Berlin, 2001.
8. R. Bröker. Constructing supersingular elliptic curves. *J. Comb. Number Theory*, 1(3):269–273, 2009.
9. A. Childs, D. Jao, and V. Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *J. Math. Cryptol.*, 8(1):1–29, 2014.
10. T. Chou and C. Orlandi. The simplest protocol for oblivious transfer. In *Progress in cryptology – LATINCRYPT 2015*, pages 40–58. Cham: Springer, 2015.
11. J.-M. Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291, 2006. `https://eprint.iacr.org/2006/291`.
12. L. De Feo, D. Jao, and J. Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *J. Math. Cryptol.*, 8(3):209–247, 2014.
13. W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, IT-22(6):644–654, 1976.
14. S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. In *Advances in cryptology—CRYPTO 1982*. New York : Plenum Press, 1983.
15. S. D. Galbraith, C. Petit, and J. Silva. Identification protocols and signature schemes based on supersingular isogeny problems. In *Advances in cryptology – ASIACRYPT 2017*, volume 10624 of *Lecture Notes in Comput. Sci.*, pages 3–33. Cham: Springer, 2017.
16. P. Gaudry. Fast genus 2 arithmetic based on Theta functions. *J. Math. Cryptol.*, 1(3):243–265, 2007.
17. P. Gaudry and D. Lubicz. The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines. *Finite Fields Appl.*, 15(2):246–260, 2009.
18. S. Goldwasser and S. Micali. Probabilistic encryption. *J. Comput. Syst. Sci.*, 28:270–299, 1984.
19. R. A. Kazmi. Cryptography from post-quantum assumptions. Cryptology ePrint Archive, Report 2015/376, 2015. `https://eprint.iacr.org/2015/376`.
20. J. Kilian. Founding cryptography on oblivious transfer. In *Proceedings of the twentieth annual ACM symposium on Theory of computing—STOC 88*, pages 20–31. ACM, 1988.
21. N. Koblitz and A. Menezes. Another look at non-standard discrete log and Diffie-Hellman problems. *J. Math. Cryptol.*, 2(4):311–326, 2008.

22. S. Kunz-Jacques and D. Pointcheval. About the security of MTI/C0 and MQV. In *Security and cryptography for networks—SCN 2006*, volume 4116 of *Lectures Notes in Comput. Sci.*, pages 156–172. Berlin: Springer, 2006.
23. P. L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Math. Comput.*, 48:243–264, 1987.
24. M. Naor and B. Pinkas. Efficient oblivious transfer protocols. In *Proceedings of the 12th annual ACM-SIAM symposium on discrete algorithms (SODA 2001)*, pages 448–457. Philadelphia, PA: SIAM, Society for Industrial and Applied Mathematics; New York, NY: ACM, Association for Computing Machinery, 2001.
25. M. Naor and B. Pinkas. Computationally secure oblivious transfer. *J. Cryptology*, 18(1):1–35, 2005.
26. C. Peikert, V. Vaikuntanathan, and B. Waters. A framework for efficient and composable oblivious transfer. In *Advances in Cryptology—CRYPTO 2008*, volume 5157 of *Lecture Notes in Comput. Sci.*, pages 554–571. Springer, Berlin, Heidelberg, 2008.
27. C. Petit. Faster algorithms for isogeny problems using torsion point images. In *Advances in cryptology – ASIACRYPT 2017*, volume 10625 of *Lecture Notes in Comput. Sci.*, pages 330–353. Cham: Springer, 2017.
28. M. O. Rabin. How to exchange secrets by Oblivious Transfer. Technical Report TR-81, Harvard Aiken Computation Laboratory, 1981.
29. J. Renes, P. Schwabe, B. Smith, and L. Batina. $\mu$Kummer: efficient hyperelliptic signatures and key exchange on microcontrollers. In *Cryptographic Hardware and Embedded Systems – CHES 2016*, volume 9813 of *Lecture Notes in Comput. Sci.*, page 20, Santa Barbara, United States, Aug. 2016. IACR, Springer-Verlag.
30. A. Rostovtsev and A. Stolbunov. Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Report 2006/145, 2006. `https://eprint.iacr.org/2006/145`.
31. P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.
32. J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.
33. A. Stolbunov. Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves. *Adv. Math. Commun.*, 4(2):215–235, 2010.
34. S. Tani. Claw finding algorithms using quantum walk. *Theoretical Computer Science*, 410(50):5285 – 5297, 2009. Mathematical Foundations of Computer Science (MFCS 2007).
35. D. Unruh. Non-interactive zero-knowledge proofs in the quantum random oracle model. In E. Oswald and M. Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015*, volume 9057 of *Lecture Note in Comput. Sci.*, pages 755–784, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.
36. J. Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci., Paris, Sér. A*, 273:238–241, 1971.
37. Q.-H. Wu, J.-H. Zhang, and Y.-M. Wang. Practical t-out-n oblivious transfer and its applications. In *Information and Communications Security – ICICS 2003*, volume 2836 of *Lecture Notes in Comput. Sci.*, pages 226–237, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.
38. Y. Yoo, R. Azarderakhsh, A. Jalali, D. Jao, and V. Soukharev. A post-quantum digital signature scheme based on supersingular isogenies. In A. Kiayias, editor, *Financial Cryptography and Data Security*, volume 10322 of *Lecture Note in Comput. Sci.*, pages 163–181, Cham, 2017. Springer International Publishing.

# A Hardness of 2-inv-CDHP in the generic group model

We follow the notations of [22], to which we refer for more details. Let $G$ be a group of prime order $p$ and $g$, $g^{x_0}$, $g^{x_1}$ three distinct group elements, different from $e = g^0$. The goal of an attacker on the 2-inv-CDHP problem is to find three non-neutral elements $Y = g^{y_0}$, $Z = g^{y_1}$, $X = g^{y_2}$ such that $Y^{x_0} = Z^{x_1} = X$; this corresponds to the modular equations

$$y_2 = x_0 y_0 = x_1 y_1 \mod p, \quad y_2 \neq 0 \mod p.$$

We observe that a uniformly random triplet $(y_0, y_1, y_2) \in \mathbb{Z}/p\mathbb{Z}$ satisfies these conditions with probability $\frac{p-1}{p^3} \leq p^{-2}$.

In the generic group model, the attacker starts with the sole knowledge of the group order and of $(r_0, r_1, r_2, r_3) = (\sigma(g^0), \sigma(g), \sigma(g^{x_0}), \sigma(g^{x_1}))$, and his goal is to produce $r_X, r_Y, r_Z \in I \setminus \{r_0\}$ such that $(\sigma^{-1}(r_Y))^{x_0} = (\sigma^{-1}(r_Z))^{x_0} = \sigma^{-1}(r_X)$. Any query to the generic group oracle necessarily involves either previously unseen elements of $I$ or previously obtained values. Each time a previously unseen element $r_j$ of $I$ is introduced as input to the oracle, we note $x_j = \log_{[g]}(\sigma^{-1}(r_j))$, where the index $j$ means that it is the $(j-3)$-th such introduced element. Any output of the oracle is thus of the form $\sigma(g^{F(x_0,x_1,x_2,\dots)})$ where $F$ is an affine polynomial in $(\mathbb{Z}/p\mathbb{Z})[X_0, X_1, X_2, \dots]$, known to the attacker. We assume that the last three queries to the oracle are the attacker's answers, i.e. are $(1, r_X, 0, \_)$, $(1, r_Y, 0, \_)$, and $(1, r_Z, 0, \_)$.

Let $F_0 = 0, F_1 = 1, F_2 = X_0, F_3 = X_1$. After $q_G$ oracle queries, the attacker knows the representation of $n$ group elements of the form $g^{F_k(x_0,x_1,x_2,\dots)}$ for a number $n$ of distinct affine polynomials in variables $X_0, X_1, \dots, X_N$, where $N$ is bounded by $2q_G + 2$ (at most two new variables for each query). This family of polynomials corresponds to the oracle outputs, but also includes the polynomials $X_2, \dots, X_N$ corresponding to the introduced elements $r_2, \dots, r_N$; thus an upper bound on $n$ is $3q_G + 4$. Since there are no affine polynomials over $\mathbb{Z}/p\mathbb{Z}$ solutions to the equations

$$P_2 = X_0 P_0 = X_1 P_1 \neq 0,$$

if all the values $(F_k(x_0, \dots, x_N))$, $0 \leq k < n$, are distinct, then the probability of success is equal to $(p-1)/p^3$. And the probability, for $(x_0, \dots, x_N)$ uniformly distributed in the set of tuples of $(\mathbb{Z}/p\mathbb{Z})^N$ without repetition, that all the values $(F_k(x_0, \dots, x_N))_{0 \leq k \leq n}$ are distinct is itself bounded below by $1 - n^2/2p$, hence the result of Theorem 1.

# B A hypothetical isogeny-based signature scheme

Isogeny-based cryptography is still recent, and currently does not offer many functionalities. In particular, it lacks an efficient signature scheme. The proposals of [15] and [38] rely on the Unruh transform (the post-quantum analog of the Fiat-Shamir transform, see [35]) applied to zero-knowledge authentification schemes, and are not considered as practical even by their authors.

We investigate in this section a hypothetical short signature scheme, that works under the assumption that the Decisional Supersingular Isogeny problem is efficiently solvable while its computational version remains intractable. It seems very unlikely that such a situation happens in the future; however, this is more or less the case in the group setting. Indeed, pairing-friendly elliptic curves provide instances of gap-Diffie-Hellman groups, i.e. groups where the decisional Diffie-Hellman problem is easy but the computational Diffie-Hellman problem is hard. Our construction is somehow inspired by the short signature scheme of [7] for these groups. Actually, we provide below two protocols, depending on whether it is the DSSI problem or its extended version (defined in Sect. 5.1) that is easily solvable.

### B.1 The easy DSSI case

We first assume that we have an algorithm that solves efficiently the decisional supersingular isogeny problem: given two supersingular curves $E_0$ and $E_1$ defined over $\mathbb{F}_{p^2}$ and a smooth integer $d$ (in what follows, $d = 2^n$ or $3^m$), where $d$ is in the order of $\sqrt{p}$, it determines if $E_0$ and $E_1$ are $d$-isogenous. Besides that, we still assume that the CSSI problem, i.e. recovering the isogeny between $E_0$ and $E_1$, is hard.

$$\begin{tikzcd}
 & E_A \simeq E/\langle R_A \rangle \arrow[dr, dotted] & \\
E, P, Q \arrow[ur, "\phi_A"] \arrow[dr, "\phi_M"'] & & \begin{array}{l} E'_M \simeq E_M/\langle \phi_M(R_A) \rangle \\ \simeq E_A/\langle \phi_A(P + H(M)\,Q) \rangle \end{array} \\
 & E_M \simeq E/\langle P + H(M)\,Q \rangle \arrow[ur, dotted] &
\end{tikzcd}$$

**Fig. 11.** Signature scheme for the easy DSSI case

- Parameter generations: Alice chooses security parameters $n, m$ such that $2^n \approx 3^m$, a supersingular curve $E$ defined over a finite field $\mathbb{F}_{p^2}$ such that $E[2^n 3^m] \subset E(\mathbb{F}_{p^2})$, and two points $P, Q$ generating $E[3^m]$. She also chooses a cryptographic hash function $H : \{0,1\}^* \to \mathbb{Z}/3^m\mathbb{Z}$.
  She selects a random cyclic subgroup $\langle R_A \rangle \subset E[2^n]$ of order $2^n$, and computes $E_A \simeq E/\langle R_A \rangle$. Her private key is $R_A$; her public key is $(E, P, Q, E_A, H)$.

- Signature: to sign a message $M$, Alice computes the curve $E_M \simeq E/\langle P + H(M)\,Q\rangle$ and the associated isogeny $\phi_M : E \to E_M$. Then she computes the curve $E'_M \simeq E_M/\langle\phi_M(R_A)\rangle$.
  The signature of the message $M$ is $sig(M) = (E_M, E'_M)$.
- Verification: upon receiving $M$ and a couple $sig = (\mathcal{E}, \mathcal{E}')$, Bob checks that $\mathcal{E}$ is isomorphic to $E/\langle P+H(M)\,Q\rangle$. Using an algorithm for the DSSI problem, he also verifies that $\mathcal{E}'$ is $2^n$-isogenous to $\mathcal{E}$ and $3^m$-isogenous to $E_A$.

Contrarily to other isogeny-based protocols, in this scheme Alice does not publish the image by $\phi_A : E \to E_A$ of the basis points $P, Q$. Otherwise, anyone could sign a message $M$ by computing $E'_M \simeq E_A/\langle\phi_A(P) + H(M)\,\phi_A(Q)\rangle$.

### B.2 The hard DSSI case

In the SIDH key exchange or in our OT scheme, there is always extra information given by the images of basis points. Thus it is conceivable that there exists an algorithm that solves the extended decisional supersingular isogeny problem of Sect. 5.1, while the DSSI problem remains hard. The previous protocol cannot be directly adapted; we present below a somewhat less elegant signature scheme for this new situation. In particular, it requires to work with a supersingular elliptic curve whose order is divisible by powers of three different primes (let us say $2^n$, $3^m$ and $5^\ell$ to fix notations) instead of just two.

$$\begin{tikzcd}
 & E_A \simeq E/\langle R_A\rangle, U, V \arrow[dr, dotted, "\phi'_M"] & \\
E, P, Q \arrow[ur, "\phi_A"] \arrow[dr, "\phi_M"'] & & \begin{array}{l} E'_M \simeq E_M/\langle\phi_M(R_A)\rangle \\ \simeq E_A/\langle\phi_A(P+H(M)\,Q)\rangle, \\ \phi'_A(Y), \phi'_A(Z), \phi'_M(U), \phi'_M(V) \end{array} \\
 & E_M \simeq E/\langle P+H(M)\,Q\rangle, Y, Z \arrow[ur, dotted, "\phi'_A"'] &
\end{tikzcd}$$

**Fig. 12.** Signature scheme for the hard DSSI case

- Parameter generations: Alice chooses security parameters $n, m, \ell$ such that $2^n \approx 3^m \approx 5^\ell$, a supersingular curve $E$ defined over a finite field $\mathbb{F}_{p^2}$ such that $E[2^n3^m5^\ell] \subset E(\mathbb{F}_{p^2})$, and two points $P, Q$ generating $E[3^m]$. She also chooses a cryptographic hash function $H : \{0,1\}^* \to \mathbb{Z}/3^m\mathbb{Z}$.

She selects a random cyclic subgroup $\langle R_A \rangle \subset E[2^n]$ of order $2^n$, and computes $E_A \simeq E/\langle R_A \rangle$ and the associated isogeny $\phi_A : E \to E_A$; she also selects a random basis $(U, V)$ of $E_A[2^n]$. Her private key is $R_A$; her public key is $(E, P, Q, E_A, U, V, H)$.

- Signature: to sign a message $M$, Alice computes the curve $E_M \simeq E/\langle P + H(M)Q \rangle$ and the associated isogeny $\phi_M : E \to E_M$. Then she computes the curve $E'_M \simeq E_M/\langle \phi_M(R_A) \rangle \simeq E_A/\langle \phi_A(P + H(M)Q) \rangle$ and the associated isogenies $\phi'_A : E_M \to E'_M$ and $\phi'_M : E_A \to E'_M$.
  She chooses a basis $(Y, Z)$ of $E_M[5^\ell]$. The signature of the message $M$ is $sig(M) = (E_M, Y, Z, E'_M, \phi'_A(Y), \phi'_A(Z), \phi'_M(U), \phi'_M(V))$.
- Verification: upon receiving $M$ and a tuple $sig = (\mathcal{E}, Y, Z, \mathcal{E}', Y', Z', U', V')$, Bob checks that $\mathcal{E}$ is isomorphic to $E/\langle P + H(M)Q \rangle$ and that $\langle Y, Z \rangle = \mathcal{E}[5^\ell]$, $\langle Y', Z' \rangle = \mathcal{E}'[5^\ell]$, $\langle U', V' \rangle = \mathcal{E}'[2^n]$. Using an algorithm for the XDSSI problem, he also verifies the existence of an isogeny $\mathcal{E} \to \mathcal{E}'$ of degree $2^n$ sending $(Y, Z)$ to $(Y', Z')$, and of an isogeny $E_A \to \mathcal{E}'$ of degree $3^m$ sending $(U, V)$ to $(U', V')$.