Revisiting SIOT protocol with new security assumptions

Paulo Barreto [1], Gláucio de Oliveira [2], Waldyr Benits [3]

1 https://orcid.org/0000-0001-8832-3071 and pbarreto@uw.edu
2 https://orcid.org/0009-0004-2534-8721 and glaucioaorj@gmail.com
3 Naval Postgraduate Institute, Brazilian Navy, Brazil and Waldyrbenits@gmail.com

Abstract: *Oblivious Transfer* is one of the most important building blocks in cryptography and useful for building secure protocols. With the advent of quantum computing there was a boost in research and development of cryptographic protocols resistant to quantum computer processing. Thus, in 2018, the SIOT (Supersingular Isogeny *Oblivious Transfer*) protocol was presented as the first post-quantum cryptographic OT scheme based on supersingular elliptic curve isogenies. Initially, an OT scheme was created combined with the cryptographic primitives of the SIDH (Supersingular Isogeny *Diffie-Hellman*) protocol. Furthermore, the SIOT protocol was built in its simplest configuration against semi-honest adversaries. However, it was subjected to scrutiny that resulted in the need to develop new security proofs. Almost in parallel, new and efficient cryptanalytic attacks emerged on the SIDH protocol, which consequently compromised the SIOT security structure. Thus, the new definitions of security proofs encompassed the compatibility of certain parameters of the OT functionality of the SIOT protocol itself with security assumptions of computational isogeny problems. After that, the security countermeasures from M-SIDH (Masked-Supersingular Isogeny *Diffie-Hellman*) protocol were analysed and implemented into SIOT protocol. Therefore, we propose an OT protocol based on isogenies of elliptic curves and with resistance to quantum attacks.

1. Introduction

The first notion of OT was proposed in [1]. In general, in an $\binom{2}{1}$-OT protocol, a sender sends two messages, say m_a and m_b, and the receiver chooses only one of them (for example, the receiver chooses m_a. At the end of the protocol, the sender does not know which of the messages were chosen, and the receiver learns nothing about the other message (in this case, m_b). OT is one of the most important and basic building blocks of cryptographic protocols whose applications can be seen in electronic auctions [2,3], contract signing [4, 5, 6] and general secure Multi-Party Computation (MPC) [7, 8]. Some OT cryptographic protocols were based on assumptions from Decisional *Diffie–Hellman* problems [9,10,11,12,13,14]. However, with the advent of quantum computing, these structures will be submitted to quantum attacks in polynomial time [15,16]. Hence, many papers have introduced OT in the context of quantum cryptography [17,18,19,20,21,22,23], where legitimate users manipulate quantum states. Additionally, the *post-quantum* OT research has gradually increased over time. New OT buildings have migrated to other new assumptions of mathematical problems based on the theory of codes [24,25,26,27,28], lattices [29,30, 31,32] and isogenies [33,34,35,36]. Therefore, OT has received considerable attention in the cryptographic literature.

Motivation. Despite the attacks CD-MM-R [37,38, 39] in exploring the images of torsion points and degrees of secret isogeny that determined the insecurity of the SIDH/SIKE schemes [40,41] and considering that other schemes based on isogenies [42,43,44,45,46,47] were not affected by these attacks, it is estimated that cryptographic builds based on isogenies is a relatively recent field compared to other areas, for instance, code theory and lattices. Thus, isogeny is a fertile area of research in cryptography. Over time, the SIOT protocol was cited by some important papers [33, 34, 35, 36, 48, 49, 50, 51, 52, 53, 54, 55, 56] and one of them [36] provided a theoretical critical analysis about security aspects. This motivated actions of corrections and improvements to the SIOT protocol. Furthermore, the paper of [57] implemented countermeasures of the attacks on the SIDH protocol and offered a reasonable alternative for repairing the SIOT protocol. Thus, important modifications were implemented in this paper. Recently, the paper of [58] claims a new polynomial-time attack applied to M-SIDH. The basic idea is to construct an auxiliary isogeny ψ related to an isogeny φ to be discovered, independently of the masking of the images of the torsion points. In other words, it is a generalisation of the "lollipop attack" described in [57]. Thus, according to a preliminary analysis in [59], apparently the tweaks to SIDH would not be enough to make it a secure protocol. However, the general case of M-SIDH has not yet been resolved. Finally, regarding the considerable increase in the efficiency cost of the SIOT protocol, due to such modifications,

[60] summarises the history of other cryptographic protocols with initial security and performance problems that were solved with the gradual evolution of computational resources and *mutatis mutandis* actions over time.

Contribution. Since 2018 [61], the SIOT is the first post-quantum OT cryptographic protocol based on isogenies of supersingular elliptic curves. Then, the purpose of this paper is to represent the SIOT with the necessary modifications to the security proofs due to the critical analysis in [36] and the attacks CD-MM-R [37,38,39] on the SIDH protocol. It should be noted that the process of building the SIOT protocol aimed at the simplest possible post-quantum OT cryptographic scheme. Hence, our protocol is inspired by the constructions of [14,40] and the security of the protocol depends on the assumptions of computational isogeny problems compatible with the properties of the OT and the countermeasures suggested in [57]. Furthermore, the security proof of our OT protocol also contains a random Oracle model making it compatible with the security concepts defined in [62].

Related work. The scheme in [49] presented research on the elaboration of an OT protocol that makes SIOT compatible with the studies in [63], i.e., the SIOT structure was extended to supersingular hyperelliptic curves with characteristic 2. The work in [34] adopted and adapted the techniques and concepts of the SIOT protocol to develop a UC-OT framework based on cryptography with isogenies between supersingular elliptic curves. Thus, they used a random Oracle model instead of the *coin flip* protocol to obtain U and V points. However, they stated that these approaches, i.e., both the random Oracle model and the *coin flip* protocol, are equivalent with respect to the security of the procedure in obtaining the mentioned points.

Outline. This paper is organised as follows: Section 2 describes the SIOT protocol. In section 3, we discuss security aspects from $\binom{2}{1}$-SIOT. In Section 4, a preliminary performance estimate between the SIOT protocol with some similar OT protocols and the M- SIDH protocol that represents the benchmark in the new security implementation. Finally, we conclude in Section 5. In addition, we use Appendix A to introduce some crucial background about OT. In Appendix B, we present some concepts of isogenies. After that, in Appendix C, there is a simplified presentation of the M-SIDH [57].

2. The SIOT protocol

In this Section, the SIOT protocol will be shown. For readers unfamiliar with issues of OT protocol, Isogeny and modifications implemented in [57] to ensure the security of SIOT, the Appendices A, B and C are suggested.

2.1 Notations

The cryptographic primitives of the SIDH protocol from [40] and the modifications proposed in [57] were used. Thus, the following notations will be described below.

i. $M, K, C \rightarrow$ Set of all plaintexts, keys and ciphertexts with binary strings of fixed length, respectively.

ii. $\lambda \rightarrow$ Security parameter, where $t = t(\lambda) \in \mathbb{N}$ be an integer depending on λ.

iii. $p \rightarrow$ Prime such that $p = A \cdot B \cdot f - 1$, where A= $\prod_{i=1}^{t} \ell_i$ and B = $\prod_{i=1}^{t} q_i$ are coprime integers and ℓ_i, q_i are distinct small primes. Furthermore, $A \approx B \approx \sqrt{p}$, f is a small cofactor and p = 3 mod4.

iv. $F_{p^2} \rightarrow$ Quadratic extension of F_p, where $F_{p^2} = F_{p[x]/\langle x^2+1\rangle}$;

v. $E_0[F_{p^2}] \rightarrow$ Supersingular elliptic curve over F_{p^2} .

vi. $P_A, Q_A \rightarrow$ Points generating $E_0[A]$, i.e, $E_0[A] = \langle P_A, Q_A \rangle$.

vii. $P_B, Q_B \rightarrow$ Points generating $E_0[B]$, i.e, $E_0[B] = \langle P_B, Q_B \rangle$.

viii. $\mu \rightarrow$ Set of square roots of unity modulo $\mathbb{N}$, where $x \in \mathbb{Z}/\mathbb{N}\,\mathbb{Z}$ such that $x^2 = 1(mod\mathbb{N})$.

ix. $\eta, \rho \rightarrow$ Random integers from $\mu(B)$ and $\mu(A)$, respectively.

x. $r_A, r_B \rightarrow$ Random integers from $\mathbb{Z}/A\,\mathbb{Z}$ and $\mathbb{Z}/B\,\mathbb{Z}$, respectively.

xi. $ker(\phi) \rightarrow$ Kernel of an isogeny. It is a finite subgroup of an elliptic curve over a closed field F_{p^2}.

xii. $\phi_A, \phi_B \rightarrow$ Isogenies between E_0 and E_A, E_0 and E_B, respectively.

xiii. $\phi'_{A_i}, \phi'_B \rightarrow$ Isogenies between E_B and E_{AB_i}, where $i \in \{0,1\}$, E_A and E_{BA}, respectively.

xiv. $\phi_A(P_B), \phi_A(Q_B) \rightarrow$ Images points from P_B and Q_B points, respectively.

xv. $\phi_B(P_A), \phi_B(Q_A) \rightarrow$ Images points from P_A and Q_A points, respectively.

xvi. $G_A, H_A \rightarrow$ Masked images points from $[\eta]\phi_A(P_B)$ and $[\eta]\phi_A(Q_B)$, respectively.

xvii. $G_B, H_B \rightarrow$ Masked images points from $[\rho]\phi_B(P_A)$ and $[\rho]\phi_B(Q_A)$, respectively.

xviii. $sk_A, sk_B \rightarrow$ Sender's private key and Receiver's private key, respectively.

xix. $pk_A, \widehat{pk}_B \rightarrow$ Sender's public key and Receiver's public key, respectively.

xx. $\jmath\left(E_{AB_i}\right), \jmath(E_{BA}) \rightarrow \jmath$ -invariant of supersingular elliptic curve E_{AB_i} and E_{BA}, respectively.

xxi. $\mathcal{E}, \mathcal{D} \rightarrow$ Encryption and Decryption algorithms, respectively.

xxii. $\mathcal{H} \rightarrow$ Hash function such that $\mathcal{H} = \{\mathcal{H}_K : k \in K\}$. It is a hash function family indexed by a finite set K, where each $\mathcal{H}_k$ is a function from F_{p^2}.

2.2 Public parameters

Let E_0 be a supersingular elliptic curve defined over F_{p^2}. For convenience, assume a prime p of form $p = A \cdot B \cdot f \pm 1$, where both A and B are coprime integers and $A \approx B \approx \sqrt{p}$. Hence, this choice yields p = 3 (mod 4). The curve $E_0\left[F_{p^2}\right]$ is a randomly generated supersingular initial curve with a ring of unknown endomorphism and group order $(A \cdot B \cdot f)^2$. Set $E_0[A]$ and $E_0[B]$ generated by kernel $\langle P_A, Q_A \rangle$ and $\langle P_B, Q_B \rangle$, respectively. The public parameters are $E_0, p, A, B, P_A, Q_A, P_B, Q_B$.

Remark 1. Recall that $A \approx B \approx \sqrt{p}$ condition remains due to the Petit's attack demonstrated by [64] in exploiting the knowledge of the endomorphism of E_0 and the torsion point information.

Remark 2. A trusted third party should use the MPC techniques described in [65] to generate a random supersingular initial E_0 curve with an unknown endomorphism ring. After that, the long random walk used should be deleted.

2.3 Preliminaries

1. Let $(\mathcal{E}, \mathcal{D})$ be a symmetric encryption scheme according to definitions 1 and 2 of [14]. The shared symmetric key is the value of the $\jmath$-invariant between two supersingular and isomorphic [1] elliptic curves. We will see in Figure 1 that the $\jmath$-invariant will be submitted to hash function $\mathcal{H} = \{\mathcal{H}_K : k \in K\}$ indexed by a finite set K, where each $\mathcal{H}_k$ is a function of F_{p^2};

2. Alice wants to encrypt two messages $m_0, m_1 \in M$ and send them to Bob. In turn, Bob will decrypt only one of these two messages, and Alice will not be aware of his choice.

3. Alice and Bob use a *coin-flipping* protocol from [66] to share a single uniform random string of ω bits. This ensures that neither Alice nor Bob can guess in advance or control the value of ω. Thus, they must use, for instance, a hash function in this bit string to get the points U and V.

4. The SIOT protocol should use the countermeasures suggested in [57], i.e., the torsion image points generated by Alice and Bob will be masked to avoid the CD-MM-R attack [37, 38, 39]. More details about this masking process can be recalled in Appendix C.

5. Some points with coordinates in a sufficiently large field E[ℓ] looks like a 2-dimensional "vector space" over $\mathbb{Z}/\ell\,\mathbb{Z}$. Therefore, a relation between these points can be found in a pairing, according to the next proposition.

Proposition 1. Let P_1, P_2 be a basis for $E[\ell]$ and $P, Q \in E[\ell]$. Then, any points P and Q can be represented as 2-dimensional vectors,

$$P = \alpha P_1 + \beta P_2, \quad (1)$$

$Q = \gamma P_1 + \delta P_2$, where $\alpha, \beta, \gamma, \delta \in \mathbb{Z}/\ell\,\mathbb{Z}$ and

$$e_\ell(P, Q) = e_\ell(P_1, P_2)^{det\binom{\alpha \quad \gamma}{\beta \quad \delta}} \quad (2)$$

Proof. See Proposition 6.33 and Theorem 6.38 from [67].

Remark 3. det stands for the mathematical operation of Determinant.

2.4 Protocol

Figure 1 shows an abstraction of the proposed protocol in its simplest form, i.e., $\binom{2}{1}$-SIOT.

2.4.1 Generation of key pairs

Setup – Sender

1. Alice chooses randomly and secretly two integers $r_A \leftarrow \$\,\mathbb{Z}/A\,\mathbb{Z}$ and $\eta \leftarrow \$\mu(B)$;

2. She computes:

(a) $ker(\phi_A) = \langle P_A + r_A Q_A \rangle$;

(b) $\phi_A : E_0 \rightarrow E_A$;

(c) $G_A \leftarrow [\eta]\phi_A(P_B), H_A \leftarrow [\eta]\phi_A(Q_B)$;

(d) η is deleted.

3. Alice creates a pair of keys $sk_A = (\phi_A, r_A)$ and $pk_A = (E_A, G_A, H_A)$, i.e, her private and public keys, respectively.

It is denoted $E_A \simeq E_0/\langle P_A + r_A Q_A \rangle$, where $|ker(\phi_A)| = |\langle P_A + r_A Q_A \rangle| = A$, i.e, a separable [2] isogeny of degree A.

[1] See [68], Proposition III.1.4(b).

[2] See [69], Proposition 12.8.

Setup – Receiver

1. Bob chooses randomly and secretly two integers $r_B \leftarrow \$\,\mathbb{Z}/B\,\mathbb{Z}$ and $\rho \leftarrow \$\mu(A)$;

2. He computes:

(a) $ker(\phi_B) = \langle P_B + r_B Q_B \rangle$;

(b) $\phi_B: E_0 \rightarrow E_B \simeq E_0/\langle P_B + r_B Q_B \rangle$;

(c) $G_B \leftarrow [\rho]\phi_B(P_A), H_B \leftarrow [\rho]\phi_B(Q_A)$;

(d) ρ is deleted.

(e) $(U, V) \in E_B[A]$ such that

i. $U = \alpha G_B + \beta H_B$ and $V = \gamma G_B + \delta H_B$ where,

• $\alpha, \beta, \gamma, \delta \in \mathbb{Z}/A\,\mathbb{Z}$.

ii. $e(U, V) = e(G_B, H_B)^{\alpha\delta -}$ such that

• $A|\alpha\delta - \beta\gamma$ and $\delta = -\alpha$.

(f) For some secret $\sigma \in \{0,1\}$ then,

i. $\hat{G}_B = (G_B - \sigma U)$;

ii. $\hat{H}_B = (H_B - \sigma V)$.

3. Bob creates a key pair $sk_B = (\phi_B, r_B)$ and $\widehat{pk}_B = \left(E_B, \hat{G}_B, \hat{H}_B\right)$, i.e, his private and public key, respectively.

4. He sends $\widehat{pk}_B$ to Alice. Then, she checks if $\hat{G}_B, \hat{H}_B \in E_B[A]$ and $e_A\left(\hat{G}_B, \hat{H}_B\right) = e_A(P_A, Q_A)^B$. Otherwise, $\widehat{pk}_B$ will be rejected ($\perp$) and the protocol is restarted.

2.4.2 Generation of secret keys

Setup – Sender

1. Alice computes:

(a) $U, V \in E_B[A]$ such that $A|(\alpha^2 + \delta^2)$, $A|\alpha\delta$, $A \nmid \gamma$, $A \nmid \beta$ and $\beta < 0$;

(b) For all $i \in \{0,1\}$,

i. $ker\left(\phi'_{A_i}\right) = \left\langle \left(\hat{G_B} + iU\right) + r_A\left(\hat{H_B} + iV\right)\right\rangle$;

ii. $\phi'_{A_i: E_B \rightarrow E_{AB_i}}$;

iii. $j_i \leftarrow j\left(E_{AB_i}\right)$;

iv. $k_i = H(j_i)$.

Remark 4. The restriction conditions for the coefficients α, β, γ and γ, when generating points U and V, for both Sender and Receiver will be demonstrated in Section 3.

Setup – Receiver

1. Bob computes:
(a) $ker(\phi'_B) = \langle G_A + r_B H_A \rangle$;

(b) $\phi'_B: E_A \rightarrow E_{BA}$;

(c) $j_\sigma \leftarrow j(E_{BA})$;

(d) k_σ = H(j_σ).

2.4.3 Encryption and Decryption

Setup – Sender

1. For all $i \in \{0,1\}$, Alice encrypts m_i. Then, $c_i \leftarrow E(k_i, m_i)$;
2. She sends (pk_A, c_0, c_1) to Bob.

Setup – Receiver

1. Upon receiving pk_A, Bob checks if $G_A, H_A \in E_A[B]$ and $e_B(G_A, H_A) = e_B(P_B, Q_B)^A$. Otherwise, that public key will be rejected ($\perp$).
2. He decrypts and gets $m_\sigma \leftarrow D(k_\sigma, c_\sigma)$.

Remark 5. Bob receives both of Alice's ciphertexts, along with her public key, which allows him to be sure that the ciphers he receives are from Alice. Hence, Alice's public key authenticates the origin of the ciphertexts

Figures 2 and 3 show the commutative diagrams of the $\binom{2}{1}$-SIOT protocol. It should be noted that there is commutativity only when both σ and i values are equal.

Supersingular Isogeny Oblivious Transfer (SIOT)

Sender		**Receiver**
Input: $m_0, m_1 \in \mathcal{M}$		Input: None
Output: None		Output: m_σ
$r_A \leftarrow\$ \mathbb{Z}/A\mathbb{Z}$		$r_B \leftarrow\$ \mathbb{Z}/B\mathbb{Z}$
$\phi_A : E_0 \rightarrow E_A$		$\phi_B : E_0 \rightarrow E_B$
$E_A \cong E_0/\langle P_A + r_A Q_A \rangle$		$E_B \cong E_0/\langle P_B + r_B Q_B \rangle$
$\eta \leftarrow\$ \mu(B)$		$\rho \leftarrow\$ \mu(A)$
$G_A \leftarrow [\eta]\phi_A(P_B); H_A \leftarrow [\eta]\phi_A(Q_B)$		$G_B \leftarrow [\rho]\phi_B(P_A); H_B \leftarrow [\rho]\phi_B(Q_A)$
η is deleted		ρ is deleted
$\mathsf{pk}_A \leftarrow (E_A, G_A, H_A)$		
		$U, V \in E_B[A]$ such that,
		$U = \alpha G_B + \beta H_B, V = \gamma G_B + \delta H_B$ where,
		$\alpha, \beta, \gamma, \delta \in \mathbb{Z}/A\mathbb{Z}$ *and*
		$e(U,V) = e(G_B, H_B)^{\alpha\delta - \beta\gamma}$ such that
		$A \mid (\alpha\delta - \beta\gamma)$ and $\delta = -\alpha$ and
		For some $\sigma \in \{0,1\}$ then,
		$\hat{G}_B \leftarrow (G_B - \sigma U)$
		$\hat{H}_B \leftarrow (H_B - \sigma V)$
	$\xleftarrow{\hat{\mathsf{pk}}_B}$	$\hat{\mathsf{pk}}_B \leftarrow (E_B, \hat{G}_B, \hat{H}_B)$
If $\hat{G}_B, \hat{H}_B \notin E_B[A]$ *and*		
$e_A(\hat{G}_B, \hat{H}_B) \neq e_A(P_A, Q_A)^B$ then,		
abort $(\perp)$.		
$U, V \in E_B[A]$ such that,		
$A \mid (\alpha^2 + \delta^2)$, $A \mid \alpha\delta$, $A \nmid \gamma$, $A \nmid \beta$, *where* $\beta < 0$.		
For all $i \in \{0,1\}$, $\phi'_{A_i} : E_B \rightarrow E_{AB_i}$		
$E_{AB_i} \cong E_B/\langle (\hat{G}_B + iU) + r_A(\hat{H}_B + iV) \rangle$		
$k_0 = \mathcal{H}(\jmath(E_{AB_0})) \therefore c_0 \leftarrow \mathcal{E}_{k_0}(m_0)$		
$k_1 = \mathcal{H}(\jmath(E_{AB_1})) \therefore c_1 \leftarrow \mathcal{E}_{k_1}(m_1)$		
	$\xrightarrow{(\mathsf{pk}_A, c_0, c_1)}$	If $G_A, H_A \notin E_A[B]$ *and*
		$e_B(G_A, H_A) \neq e_B(P_B, Q_B)^A$ *then*,
		abort $(\perp)$.
		$\phi'_B : E_A \rightarrow E_{BA}$
		$E_{BA} \cong E_A/\langle G_A + r_B H_A \rangle$
		$k_\sigma = \mathcal{H}(\jmath(E_{BA}))$
		$m_\sigma \leftarrow \mathcal{D}_{k_\sigma}(c_\sigma)$.

Fig. 1: $\binom{2}{1}$-SIOT protocol

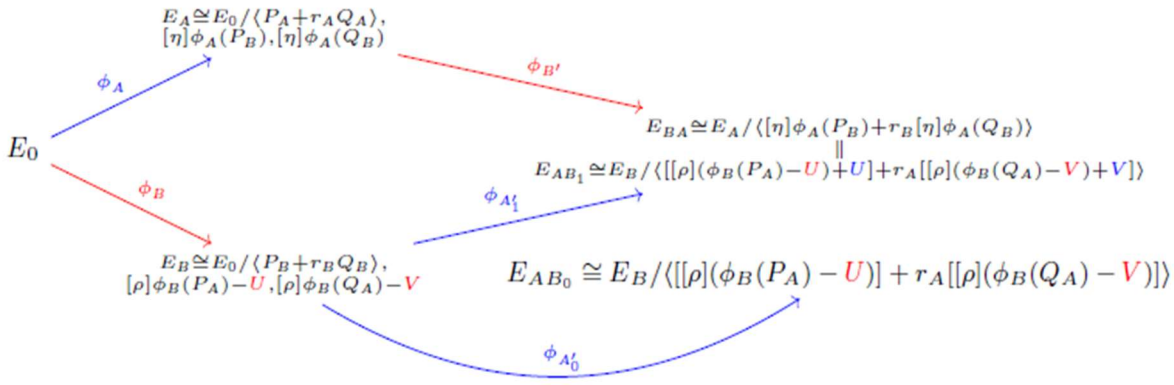


Fig. 2: Commutativity in $\binom{2}{1}$-SIOT with $\sigma = i = 1$.

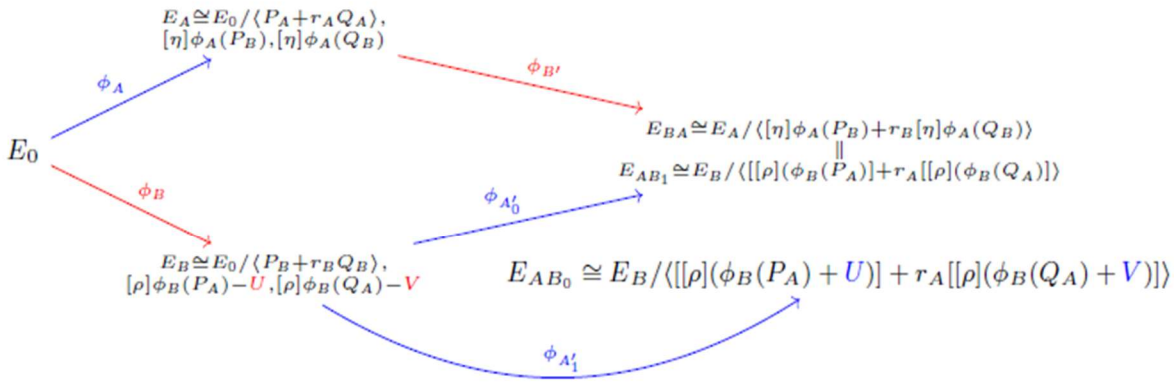


Fig. 3: Commutativity in $\binom{2}{1}$-SIOT with $\sigma = i = 0$.

3 Security analysis of the SIOT protocol

In this section it will be seen that the security of the SIOT protocol was based on the compatibility of computational assumptions and concepts elaborated in [40, 57,62]. It is worth recalling that Appendix A presents in a simplified form the OT protocol from [14] which served as the initial inspiration for the SIOT protocol due to its relative simplicity.

Remark 6. As for the requirements[3] of the initial E_0 curve for the SIOT protocol to be secure, in [58] the authors claim that such requirements are not sufficient to contain their attack. Although, the MPC protocol ensures a high probability of generating an E_0 curve without a backdoor.

3.1 Computational problems of isogenies between supersingular elliptic curves

Now, as mentioned previously, the computational assumptions that ensure the security of the SIOT protocol will be seen. According to [57], the computational problem 1 underlies the security of the M-SIDH[4] protocol.

Computational Problem 1. Let A = $\prod_{i=1}^{t} \ell_i$ and let B = $\prod_{i=1}^{t} q_i$ be two large coprime integers, let f be a small cofactor such that $p = A \cdot B \cdot f - 1$ is a prime, with $A \approx B \approx \sqrt{p}$. Let E_0 be a supersingular elliptic curve defined over F_{p^2}, with group order $(A \cdot B \cdot f)^2$. Set $E_0[A] = \langle P_A, Q_A \rangle$ and set $E_0[B] = \langle P_B, Q_B \rangle$. Let $\phi_A: E_0 \to E_A$ and let $\phi_B: E_0 \to E_B$ be a uniformly random A-isogeny and a uniformly random B-isogeny, respectively. Let η and ρ be uniformly random elements of $\mu(B)$ and $\mu(A)$, respectively. Given E_0 and the public keys $\big(E_A, [\eta]\phi_A(P_B), [\eta]\phi_A(Q_B)\big)$ and $\big(E_B, [\rho]\phi_B(P_A), [\rho]\phi_B(Q_A)\big)$, compute ϕ_A and ϕ_B.

Furthermore, the SIOT protocol is a variant of SIDH/M-SIDH. Thus, to ensure the security of the SIOT protocol, it was necessary to adapt the computational assumptions elaborated in [40] and, as will be seen in the next section, make them compatible with the security concepts presented in [62]. It is important to recall that the main countermeasure to the CD-MM-R attacks [37,38,39] is to ensure that the direct images $\phi_A(P_B)$, $\phi_A(Q_B)$, $\phi_B(P_A)$ and $\phi_B(Q_A)$ should not be available to an adversary. Therefore, let a supersingular curve E_0 over F_{p^2} together with independent bases $\{P_A, Q_A\}$ and $\{P_B, Q_B\}$ of $E_0[A]$ and $E_0[B]$, respectively:

Computational Problem 2. Let $E_A\big[F_{p^2}\big]$ be another supersingular curve. Decide whether E_A is A-isogenous to E_0.

Computational Problem 3. Let $\phi_A: E_0 \to E_A$ be an isogeny whose kernel is $R_A = \langle P_A + [r_A]Q_A \rangle$, where r_A is chosen at random from $\mathbb{Z}/A\,\mathbb{Z}$ and not divisible by A. Given the public key $\big(E_A, [\eta]\phi_A(P_B), [\eta]\phi_A(Q_B)\big)$, find the generator R_A of $\langle P_A + [r_A]Q_A \rangle$.

Computational Problem 4. Let $\phi_A: E_0 \to E_A$ be an isogeny whose kernel is $R_A = \langle P_A + [r_A]Q_A \rangle$, where r_A is chosen at random from $\mathbb{Z}/A\,\mathbb{Z}$ and not divisible by A and let $\phi_B: E_0 \to E_B$ be an isogeny whose kernel is $R_B = \langle P_B + [r_B]Q_B \rangle$, where r_B is chosen at random from $\mathbb{Z}/B\,\mathbb{Z}$ and not divisible by B. Given the public keys $(E_A, [\eta]\phi_A(P_B), [\eta]\phi_A(Q_B))$ and $\big(E_B, [\rho]\phi_B(P_A), [\rho]\phi_B(Q_A)\big)$. Determine the $\jmath$ − invariant of

$$E_0/\langle P_A + [r_A]Q_A, P_B + [r_B]Q_B \rangle.$$

Computational Problem 5. Given a tuple sampled with probability 1/2 from one of the following two distributions:

1. $(E_A, E_B, [\eta]\phi_A(P_B), [\eta]\phi_A(Q_B), [\rho]\phi_B(P_A)$

$, [\rho]\phi_B(Q_A), E_{AB})$, where $E_A, E_B, [\eta]\phi_A(P_B)$, $[\eta]\phi_A(Q_B), [\rho]\phi_B(P_A)$ and $[\rho]\phi_B(Q_A)$ are as in the Computational Problem 4 then,

$$E_{AB} \cong E_0/\langle P_A + [r_A]Q_A, P_B + [r_B]Q_B \rangle.$$

2.$(E_A, E_B, [\eta]\phi_A(P_B), [\eta]\phi_A(Q_B), [\rho]\phi_B(P_A),$

$[\rho]\phi_B(Q_A), E_C)$, where $E_A, E_B, [\eta]\phi_A(P_B)$, $[\eta]\phi_A(Q_B), [\rho]\phi_B(P_A)$ and $[\rho]\phi_B(Q_A)$ are as in the Computational Problem 4 then,

$$E_C \cong E_0/\langle P_A + \hat{r}_A Q_A, P_B + \hat{r}_B Q_B \rangle$$

where $\hat{r}_A$ (respectively $\hat{r}_B$) is chosen at random from $\mathbb{Z}/A\,\mathbb{Z}$ (respectively $\mathbb{Z}/B\,\mathbb{Z}$) and not divisible by A (respectively B), determine from which distribution the tuple is sampled.

3.2 Some requirements for security analysis

A priori, any secure protocols should resist to any adversarial attack. Thus, to prove that an OT protocol is secure, [62] state that the most important requirements in any security protocol are correctness and privacy.

3.2.1 Correctness

Suppose that both Alice and Bob are honest parties taking the $\binom{2}{1}$-SIOT protocol. Let $\sigma, i \in \{0,1\}$ such that $\sigma = i$. Thus, the correctness follows the identities below.

[3] Recalling Section 2.2, remark 2.
[4] See M-SIDH in the Appendix C.

$$
\begin{aligned}
&\jmath\left(E_{AB_i}\right) \cong \\
&\jmath(E_B/\langle(G_B - \sigma U + iU) + r_A(H_B - \sigma V + iV)\rangle) \\
&\quad \cong \jmath\big(\phi_B(E_0)/([\rho]\phi_B(P_A) - \sigma U + iU) \\
&\qquad + r_A([\rho]\phi_B(Q_A) - \sigma V + iV)\big) \\
&\quad \cong \jmath(\phi_B(E_0)/\langle[\rho]\phi_B(P_A) + r_A[\rho]\phi_B(Q_A)\rangle) \\
&\quad \cong \jmath(\phi_B(E_0)/\langle[\rho]\phi_B(P_A + r_A Q_A)\rangle) \\
&\quad \cong \jmath(\phi_B(E_0)/\langle\phi_B(P_A + r_A Q_A)\rangle) \\
&\quad \cong \jmath\left(\phi'_A(\phi_B(E_0))\right) \\
&\quad \cong \jmath(\phi_A(E_0)/\langle\phi_A(P_B + r_B Q_B)\rangle) \\
&\quad \cong \jmath\left(\phi'_{A_i}(\phi_B(E_0))\right) \\
&\quad \cong \jmath(E_B/\langle[\eta]\phi_A(P_B) + r_B[\eta]\phi_A(Q_B)\rangle) \\
&\quad \cong \jmath\left(\phi'_B(\phi_A(E_0))\right) \\
&\quad \cong \jmath(E_{BA}).
\end{aligned}
$$

3.2.2 Privacy

In the $\binom{2}{1}$-SIOT protocol, Bob's choice should not be known to Alice. Moreover, at the end of the protocol, Bob will not be able to gain any knowledge about the message that he did not decrypt. It should be noted that this privacy stems from the difficulty of solving the computational problems seen in Section 3.1. Basically, an adversary is considered semi-honest in the configuration where the corrupted party correctly follows the protocol specification. Furthermore, in the malicious adversary model, the corrupted party can arbitrarily deviate from the protocol specification according to the adversary's instructions. Ideally, it is preferable to provide security in the presence of malicious adversaries, as it ensures that no adversarial attack will be successful. However, as described in [62], protocols that configure this level of security are typically much less efficient. Additionally, and intuitively, operations involving isogenies and pairings provide a relatively low efficiency. Thus, in this paper, it was decided to consider semi-honest adversaries in the design of the SIOT scheme. Finally, to ensure the privacy requirement in the SIOT protocol, Theorem 1 was inspired by the Definition 1 presented[5] in [62] and elaborated as follows[6]:

Theorem 1. Assume that Computational Problems 2, 3, 4 and 5 are hard in a group $E_0[F_{p^2}]$. Then, $\binom{2}{1}$-SIOT protocol ensures privacy between two parties.

Proof. The proof is to adapt Definition 1 of [62] for compatibility with the computational problems mentioned in section 3.1. Let two messages, m_0 and m_1, between two parts (Alice and Bob). Then, $\binom{2}{1}$-SIOT protocol is private if the following requirements are valid:

i. Non-triviality: If Alice and Bob follow the protocol correctly then, after an execution in which Alice has for input any $m_0, m_1 \in M$ and output c_i for all $i \in \{0,1\}$. Bob has input some $\sigma \in \{0,1\}$ and output m_σ. Thus, non-triviality follows from the fact that

$$
(m_0, m_1, \sigma) \to (i, m_\sigma) \text{ where, } For\ all\ \sigma = i \to V\acute{e}lu's^{7}\ formula\{\langle G_A + r_B H_A\rangle, E_A\} \Rightarrow E_{BA} \therefore H\big(\jmath(E_{BA})\big) \Rightarrow k_\sigma
$$

Remark 7. As notation it will be used Application of the $V\acute{e}lu'sformula \to V\acute{e}lu'sformula\{ker(\phi), E\}$;

Therefore, the non-triviality property states that Bob will always need Alice's public key, i.e., $pk_A \Leftarrow (E_A, G_A, H_A)$, to generate an isogeny such that only one of two encrypted messages will be decrypted.

ii. Privacy in the case of a semi-honest Alice: In what follows, all pairings have order A. For some $\sigma \in \{0,1\}$, Alice receives the tuple $(E_B, G_B - \sigma U, H_B - \sigma V)$. Furthermore, $e(G_B - \sigma U, H_B - \sigma V) = e(P_A, Q_A)^A$ must be valid such that Bob's choice σ is not known to Alice. Thus, it can apply a matching operation on the points $(G_B - \sigma U, H_B - \sigma V)$ to observe some mismatch, i.e, $e(G_B - \sigma U, H_B - \sigma V) = e(P_A, Q_A)^A = e(G_B, H_B)$. Recall that the points $U, V \in E_B[A]$ can be written as 2-dimensional vectors, i.e., $U = \alpha G_B + \beta H_B, V = \gamma G_B + \delta H_B$ such that $\alpha, \beta, \gamma, \delta \in \mathbb{Z}/A\,\mathbb{Z}$. Considering $\sigma = 1$, then

$$
\begin{aligned}
&e(G_B - U, H_B - V) = e(G_B, H_B - V)e(-U, H_B - V); \\
&= e(G_B, H_B)e(G_B, -V)e(-U, H_B)e(-U, -V); \\
&= e(G_B, H_B)e(G_B, -\gamma G_B - \delta H_B)e(-\alpha G_B \\
&\qquad - \beta H_B, H_B)e(U, V); \\
&= e(G_B, H_B)^{1-\delta}e(-\alpha G_B - \beta H_B, H_B)e(\alpha G_B \\
&\qquad + \beta H_B, \gamma G_B + \delta H_B); \\
&= e(G_B, H_B)^{1-\delta}e(G_B, H_B)^{-\alpha+\alpha\delta-\beta\gamma}; \\
&= e(G_B, H_B)^{1-\delta-\alpha+\alpha\delta-} \quad ; \\
&= e(G_B, H_B).
\end{aligned}
$$

Thus, it is necessary $1 - \delta - \alpha + \alpha\delta - \beta\gamma = 1(modA)$ or, equivalently, $-\delta - \alpha + \alpha\delta - \beta\gamma = 0(modA)$. In particular, for those invertible $(modA)$ it must be valid that $\alpha\delta = \delta + \alpha + \beta\gamma(modA)$.

[5] See Appendix A.2.

[6] Recalling that $[\eta]\phi_A(P_B) \leftarrow G_A$ and $[\eta]\phi_A(Q_B) \leftarrow H_A$ and, $[\rho]\phi_B(P_A) \leftarrow G_B$ and $[\rho]\phi_B(Q_A) \leftarrow H_B$.

[7] See [74], Corollary 25.1.7.

Hence, $\alpha\delta - \beta\gamma = \alpha + \delta$ then, $A|\alpha + \delta$ or, equivalently, $\delta = -\alpha$. Therefore, such conditions must be obeyed such that Alice does not find Bob's choice, i.e, the σ value. The above conditions against a semi-honest Alice imply the following computational assumption[8].

Extended Computational Problem 5

Let $\phi_B: E_0 \to E_B$ be an isogeny whose kernel is $\langle P_B + r_B Q_B \rangle$, where r_B is chosen at random from $\mathbb{Z}/B\,\mathbb{Z}$ and not divisible by B. Let the points G_B, H_B, U, V such that $\langle U, V \rangle = \langle G_B, H_B \rangle = E_B[A]$, $e(G_B, H_B) = e\big((G_B - U), (H_B - V)\big) = e(P_A, Q_A)^A$ and $e(U,V) = e(G_B, H_B)^{\alpha\delta - \beta\gamma}$,where $A|\alpha\delta - \beta\gamma$ and $\alpha = -\delta$. Given a sampled tuple with probability 1/2 from one of the following two distributions:

1.$(E_0, E_B, G_B, H_B, E_{AB})$, where
$$E_{AB} \cong E_B/\langle (G_B + r_A H_B) \rangle,$$

2. $\big(E_0, E_B, (G_B - U), (H_B - V), \tilde{E}_{AB}\big)$, where

$$\tilde{E}_{AB} \cong E_B/\langle \big[(G_B - U) + U\big] + \tilde{r}_A \big[(H_B - V) + V\big] \rangle,$$
where

r_A and $\tilde{r}_A$ are chosen randomly from $\mathbb{Z}/A\,\mathbb{Z}$ and not divisible by A.

Determine which distribution the tuple is sampled.

Thus, upon receiving Bob's public key, Alice will not be able to distinguish whether this key is defined with points U and V. Bob must ensure that $e(G_B, H_B) = e\big((G_B - U), (H_B - V)\big) = e(P_A, Q_A)^A$ and $e(U,V) = e(G_B, H_B)^{\alpha\delta -}$ [9], where $A|\alpha\delta - \beta\gamma$ and $\alpha = -\delta$. Combining the constraints of these coefficients then results in $\gamma = -\frac{\alpha^2}{\beta}$. It turns out that $V = -(\alpha/\beta)U$. Therefore, Alice does not find the value of σ and there is no apparent reduction from Extended Computational Problem 5 to the Computational Problem 4.

Remark 8. As a premise, the sender should not control the coefficient values. Otherwise, he could try to find a mismatch between his pair of points (U,V) and the points $\big(\hat{G}_B, \hat{H}_B\big)$ of the receiver of his public key $\widehat{pk}_B$ with the purpose of finding the value of σ. Thus, the following Proposition was elaborated:

Proposition 2. If Extended Computational Problem 5 holds and the shared pair of points (U,V) is generated by means of a *coin-flip* protocol, then the sender may try to control such coefficients, and he will not be able to find the value of σ.

Proof. By means, $\widehat{pk}_B$ the receiver sends to the sender one of the pairs (G_B, H_B) or $(G_B - U, H_B - V)$. Thus, upon receipt of $\hat{G}_B$ and $\hat{H}_B$ points, assume by contradiction that the sender will manipulate the coefficients α, β, γ and δ to try to find the value of σ chosen from the receiver. The algebraic developments are as follows:

$$U = \alpha \cdot \hat{G}_B + \beta \cdot \hat{H}_B;$$

$$U = \alpha \cdot (G_B - U) + \beta \cdot (H_B - V);$$

$$U = \alpha \cdot G_B - \alpha \cdot U + \beta \cdot H_B - \beta \cdot V;$$

$$U = \underbrace{\alpha \cdot G_B + \beta \cdot H_B}_{U} - (\alpha \cdot U + \beta \cdot V);$$

$$U = U - (\alpha \cdot U + \beta \cdot V);$$

$$U = U - [\alpha \cdot (\alpha \cdot G_B + \beta \cdot H_B) + \beta \cdot (\gamma \cdot G_B + \delta \cdot H_B)];$$

$$U = U - [\alpha^2 \cdot G_B + \alpha \cdot \beta \cdot H_B + \beta \cdot \gamma \cdot G_B + \beta \cdot \delta \cdot H_B];$$

$$U = U - [\alpha^2 \cdot G_B + \beta \cdot \gamma \cdot G_B + \alpha \cdot \beta \cdot H_B + \beta \cdot \delta \cdot H_B];$$

$$U = U - \left[\underbrace{(\alpha^2 + \beta \cdot \gamma)G_B + (\alpha \cdot \beta + \beta \cdot \delta)H_B}_{0}\right].$$

Thus, the following conditions must be considered to avoid the sender finding a mismatch between its pair of points (U,V) and the pair of points $\big(\hat{G}_B, \hat{H}_B\big)$

$$\begin{cases} \alpha^2 + \beta \cdot \gamma = 0 \therefore \gamma = -\dfrac{\alpha^2}{\beta}; \\ \alpha \cdot \beta + \beta \cdot \delta = 0 \therefore \alpha = -\delta. \end{cases}$$

These conditions confirm the Extended Computational Problem 5. The same result is found, when trying to observe an incompatibility with point V,

$$V = \gamma \cdot \hat{G}_B + \delta \cdot \hat{H}_B;$$

$$V = \gamma \cdot (G_B - U) + \delta \cdot (H_B - V);$$

$$V = \gamma \cdot G_B - \gamma \cdot U + \delta \cdot H_B - \delta \cdot V;$$

$$V = \underbrace{\gamma \cdot G_B + \delta \cdot H_B}_{V} - (\gamma \cdot U + \delta \cdot V);$$

$$V = V - (\gamma \cdot U + \delta \cdot V);$$
$$V = V - [\gamma \cdot (\alpha \cdot G_B + \beta \cdot H_B) + \delta \cdot (\gamma \cdot G_B + \delta \cdot H_B)];$$

$$V = V - [\alpha \cdot \gamma \cdot G_B + \beta \cdot \gamma \cdot H_B + \gamma \cdot \delta \cdot G_B + \delta^2 \cdot H_B];$$

[8] Recall that p is a prime number of the form $p = A \cdot B - 1$ and a supersingular elliptic curve E_0 over F_{p^2} with bases $\{P_A, Q_A\}$ and $\{P_B, Q_B\}$ of $E_0[A]$ and $E_0[B]$, respectively.

[9] Recall Proposition 1.

$V = V - [\alpha \cdot \gamma \cdot G_B + \gamma \cdot \delta \cdot G_B + \beta \cdot \gamma \cdot H_B + \delta^2 \cdot H_B]$;

$$V = V - \left[\underbrace{(\alpha \cdot \gamma + \gamma \cdot \delta)G_B + (\delta^2 + \beta \cdot \gamma)H_B}_{0}\right];$$

$$\begin{cases} \alpha \cdot \gamma + \gamma \cdot \delta = 0 \therefore \alpha = -\delta; \\ \delta^2 + \beta \cdot \gamma = 0 \Rightarrow \gamma = -\delta^2/\beta \therefore \gamma = -\alpha^2/\beta\,. \end{cases}$$

Therefore, if the sender controlled the coefficients α, β, γ and δ, it would not be possible to find an incompatibility and, consequently, deduce the values of σ. □

iii. Privacy in the case of a semi-honest Bob: Let E_0, E_A and E_B be three supersingular elliptic curves defined over F_{p^2} such that E_A and E_B are isogenous to E_0 and $\phi_A: E_0 \to E_A$, $\phi_B: E_0 \to E_B$ their corresponding isogenies of degrees A and B, respectively. Let $(P_A, Q_A) \in E_0[A]$, $(P_B, Q_B) \in E_0[B]$, $(U, V) \in E_B[A]$ and, for some $\sigma \in \{0,1\}$, $\hat{G}_B \leftarrow (G_B - \sigma \cdot U)$, $\hat{H}_B \leftarrow (H_B - \sigma \cdot V)$ and a randomly chosen value r_A of $\mathbb{Z}/A\,\mathbb{Z}$, where $A \nmid r_A$. Alice receives Bob's public key, i.e, $(E_B, \hat{G}_B, \hat{H}_B)$. Then, for all $i \in \{0,1\}$, it will compute the isogenies $\phi_{A_i}: E_B \to E_{AB_i} \simeq E_B/\langle (\hat{G}_B + i \cdot U) + r_A(\hat{H}_B + i \cdot V)\rangle$. Considering $\sigma = 0$, $G_B \leftarrow [\rho]\phi_B(P_A)$, $H_B \leftarrow [\rho]\phi_B(Q_A)$ and recalling that $U = \alpha \cdot G_B + \beta \cdot H_B$ and $V = \gamma \cdot G_B + \delta \cdot H_B$, Alice computes $E_{AB_0} \simeq E_B/\langle G_B + r_A \cdot H_B\rangle$ and $E_{AB_1} \simeq E_B/\langle (G_B + U) + r_A(H_B + V)\rangle$. Equivalently, $(G_B + V) + r_A(H_B + V) = (1 + \alpha + \gamma \cdot r_A) \cdot G_B + (r_A + \beta + \delta \cdot r_A)H_B$ and, by inspection, this point belongs to the kernel $\langle G_B + r_A \cdot H_B\rangle$. Then, observing the following conditions:

1. $(1 + \alpha + \gamma \cdot r_A)$ is invertible modA, i.e, if $A \nmid (1 + \alpha + \gamma \cdot r_A)$;

2. $(r_A + \beta + \delta \cdot r_A)/(1 + \alpha + \gamma \cdot r_A) = r_A(modA)$ which means $\gamma \cdot {r_A}^2 + (\alpha - \delta)r_A - \beta = 0(modA)$. This equation must have no solution, otherwise Bob will be able to compute the value of r_A. Thus, its discriminate must be less than zero, i.e, $\Delta < 0$, or equivalently, $[(\alpha - \delta)^2 + 4 \cdot \beta \cdot \gamma]/2 \cdot \gamma < 0(modA)$. Hence,

$$\Delta = \frac{(\alpha - \delta)^2 + 4 \cdot \beta \cdot \gamma}{2 \cdot \gamma} < 0(modA);$$

$$\Delta = \frac{\alpha^2 - 2 \cdot \alpha \cdot \delta + \delta^2 + 4 \cdot \beta \cdot \gamma}{2 \cdot \gamma} < 0(modA);$$

$$\Delta = \frac{(\alpha^2 + \delta^2) - 2 \cdot \alpha \cdot \delta + 4 \cdot \beta \cdot \gamma}{2 \cdot \gamma} < 0(modA);$$

$$\Delta = \frac{(\alpha^2 + \delta^2)}{2 \cdot \gamma} - \frac{2 \cdot \alpha \cdot \delta}{2 \cdot \gamma} + \frac{4 \cdot \beta \cdot \gamma}{2 \cdot \gamma} < 0(modA);$$

$$\Delta = \frac{(\alpha^2 + \delta^2)}{2 \cdot \gamma} - \frac{\alpha \cdot \delta}{\gamma} + 2 \cdot \beta < 0(modA).$$

Therefore, arbitrarily, it must be defined that $A|(\alpha^2 + \delta^2)$, $A|\alpha \cdot \delta$, $A \nmid \gamma$, $A \nmid \beta$ such that $\beta < 0$.

Extended Computational Problem 3
Let $\phi_B : E_0 \to E_B$ be an isogeny whose kernel is $\langle P_B + r_B \cdot Q_B\rangle$, where r_B is chosen at random from Z/BZ and $B \nmid rB$. Let the pair of points (U, V) $\in E_B[A]$ be such that $A \mid (\alpha^2 + \delta^2)$, $A \mid \alpha \cdot \delta$, $A \nmid \gamma$ and $A \nmid \beta$, where $\beta < 0$. Bob computes the public key $(E_B, \hat{G}_B, \hat{H}_B)$ and he must find the supersingular elliptic curves E_{AB_0} and E_{AB_1} such that $E_{AB_0} \cong E_B/\langle \hat{G}_B + r_A \cdot \hat{H}_B\rangle$ and $E_{AB_1} \cong E_B/\langle (\hat{G}_B + U) + r_A(\hat{H}_B + V)\rangle$.

There is the premise that the solution of the Computational Problem 3 will lead to the solution of the Extended Computational Problem 3. It seems unlikely that Bob will be able to compute r_A. Recalling that the j-invariants from E_{AB_0} and E_{AB_1} correspond to the two encryption keys of the messages of the protocol. The following computational problem was inspired from the IND-CPA property. A priori, in an OT protocol, the receiver must not have any knowledge about the operations and results performed by the sender. Then, the security assumption against a dishonest Bob relies on the following problem,

Extended Computational Problem 2
Let $\tilde{\phi}_B : E_0 \to \tilde{E}_B$ be an isogeny whose kernel is $\langle P_B + \tilde{r}_B Q_B\rangle$, where $\tilde{r}_B$ is chosen at random from Z/BZ and B $\nmid \tilde{r}_B$. Let the pair of points $(U, V) \in \tilde{E}_B[A]$ be such that $A \mid (\alpha^2 + \delta^2)$, $A \mid \alpha \cdot \delta$, $A \nmid \gamma$ and $A \nmid \beta$, where $\beta < 0$.

- Bob sends a supersingular elliptic curve $\tilde{E}_B$ and a pair of points $(\tilde{G}_B, \tilde{H}_B) \in \tilde{E}_B[A]$for an Oracle.
- The Oracle computes the supersingular elliptic curves $E_{AB_0} \cong \tilde{E}_B/\langle \tilde{G}_B + r_A \tilde{H}_B\rangle$ and $E_{AB_1} \cong \tilde{E}_B/\langle (\tilde{G}_B + U) + r_A(\tilde{H}_B + V)\rangle$.
- For all $\tau \in \{0,1\}$, the Oracle randomly chooses the value of the τ bit. Then, it generates a pair of supersingular elliptic curves (C_0, C_1) such that

$$(C_0, C_1) = \begin{cases} (E_{AB_0}, E_{AB_1}), if\ \tau = 0; \\ (E_{AB_1}, E_{AB_0}), if\ \tau = 1. \end{cases}$$

- Bob must decide whether τ = 0 or 1.

Considering both Bob and the Oracle execute the protocol according to its correctness and recalling that $\tilde{G}_B, \tilde{H}_B, U, V \in \tilde{E}_B[A]$ such that $\tilde{G}_B = ([\rho]\phi_B(P_A) - \sigma U)$ and $\tilde{H}_B = ([\rho]\phi_B(Q_A) - \sigma V)$ for some $\sigma \in \{0,1\}$. Thus, in an operation of OT protocol between two parties, Bob sends his public key $(\tilde{E}_B, \tilde{G}_B, \tilde{H}_B)$ and, subsequently, the pair of elliptic curves E_{AB_0} and E_{AB_1} are generated such that it is expected to be computationally infeasible for Bob to distinguish in which of these curves used the pair of points (U, V) generated from the Oracle. Then, for all $n \in N$ and for some negligible function $\epsilon(n)$, the probability of Bob deciding the correct value of the bit τ will not be greater than $1/2 + \epsilon(n)$. Furthermore, similarly to Extended Computational Problem 3, it seems to be hard to solve Extended Computational Problem 2 without computing the secret value r_A from the Oracle. There is no apparent reduction from Extended Computational Problem 2 to Computational Problem 2. Moreover, a possible solution to Extended Computational Problem 3 would imply solutions to Extended Computational Problems 2 and 5.

3.3 Summing up the conditions

We consider the conditions defined into coefficients α, β, γ and δ from the security proof from section 3.2.2. Thus, recalling these conditions and the vector structure of points U and V,

$$\begin{cases} \gamma = -\dfrac{\alpha^2}{\beta}; \\ \delta = -\alpha; \\ \gamma \neq 0 \; and \; \beta < 0. \end{cases}$$

Combining such conditions then,

$$\begin{cases} \gamma = -\dfrac{\alpha^2}{\beta}; \\ \alpha \neq 0. \end{cases}$$

Therefore, the association of Theorem 1 that defines the conditions of the above coefficients to provide privacy between sender and receiver with Computational Problem 1 ensures the security of the SIOT protocol.

4 A preliminary performance estimate between some OT protocols

To estimate the efficiency of an OT protocol, the number of rounds, bandwidth (size of keys exchanged between parties) and local computation are considered, i.e., the number of types of operations such as addition and multiplication that are normally performed faster compared to isogenies and Weil parings calculations which are slower. Then, the estimated efficiency of the SIOT protocol is described below. In Table 1, we have the number of types of operations by sender and receiver in SIDH-OT / SIDH-WSW-OT [33], SIOT and M-SIDH [57]. It is important to mention that scalar multiplications and additions with points are denoted by Multi and Add, respectively. Furthermore, calculations for isogenies and pairing are denoted by Iso and Png, respectively.

Table 1: Performance estimation between OT

	Sender			Receiver			
Protocol	**Mult**	**Add**	**Iso**	**Mult**	**Add**	**Iso**	**Png**
SIDH-OT	8	4	4	2	2	2	2
SIDH-WSW-OT	3	3	5	2	1	2	4
SIOT	3	5	3	2	4	2	3
M-SIDH	4	2	2	4	2	2	2

The SIOT protocol is a variant of the SIDH/M-SIDH protocols. Hence, the complexities of calculations in SIOT are similar to those performed in M-SIDH. An example of this, regarding bandwidth, are the sizes of public keys, i.e., due to the countermeasures suggested in [57], the SIOT protocol must use the same key sizes[10] used by M-SIDH. Furthermore, in the M-SIDH protocol the scalar multiplication to mask the torsion points was considered negligible by its authors. Then, for a simplified analysis, the complexity of this type of operation could be insignificant in the SIOT protocol as well as in the number of additional operations. Although, the SIOT protocol has practically double the number of addition operations compared to M-SIDH. It is observed that Figure 4 graphically reflects Table 1.

Remark 9. SIDH-OT and SIDH-WZW-OT are schemes based on discrete logarithms in a Diffie-Hellman problem, using double isogenies. Although these protocols do not include the countermeasures[11] suggested in [57], they were chosen for a comparative analysis to highlight the relatively simpler structure of the SIOT protocol.

[10] According to [57], this means that the size of the public keys of the SIOT protocol will be approximately 7 to 8 times larger than the keys of the SIKE protocol.

[11] If these protocols implemented countermeasures against CD-MM-R attack [37,38,39], intuitively there would be a certain increase in addition operations that for our preliminary analysis would be negligible.

Remark 10. It is noted that the number of pairings for each protocol is slightly equivalent. In a more careful analysis, the SIDH-OT protocol has a smaller number of pairings than SIOT. However, it has a greater number of rounds and isogenies operations. Finally, it is worth highlighting that the comparison of SIOT with M-SIDH only aims to estimate how much efficiency was changed in the latter.

Therefore, to estimate preliminary efficiency in the SIOT protocol, it was taken into consideration that the relatively most expensive type of operation in an isogeny-based cryptographic protocol is the calculation of high-degree isogenies. Furthermore, the number of rounds was defined as an important factor for performance analysis. Thus, the SIOT protocol has only two rounds and five isogeny calculations in its complete operation. Comparatively, this means that SIOT is slightly less efficient than M-SIDH, although it has fewer rounds. In relation to the other protocols, i.e., SIDH-WSW-OT and SIDH-OT, it seems that the efficiency of the SIOT protocol is slightly better.

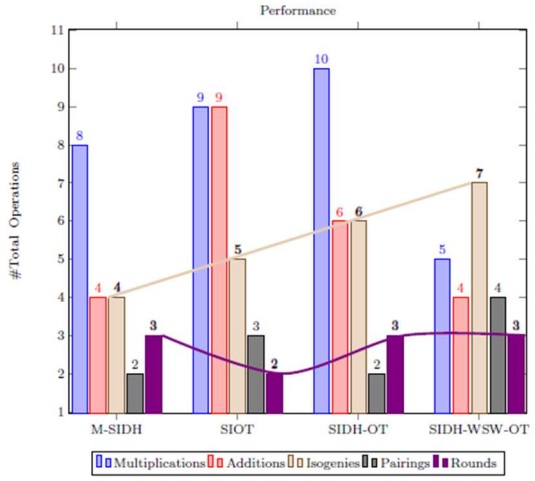


Figure 4: Performance estimation between OT protocols

5 Conclusion

This paper represents the proposal for the first post quantum OT protocol in the simplest possible construction. Calculations and assumptions of computational problems of isogenies of supersingular elliptic curves were again adapted and associated with security concepts of OT protocols to ensure the security and privacy between parties of the SIOT protocol. Although the efficiency of the SIOT has suffered considerable degradation due to the need for implementations suggested in the M-SIDH protocol, it is known that history has shown that some cryptographic protocols initially released in the past have had several changes implemented over time, in order to correct security compromises or efficiency improvements. Therefore, it is expected that this research will serve as a motivation and direction for further development of post-quantum OT cryptographic protocols.

Acknowledgments

We would like to thank Disnei Vieira Salles[12], senior mathematician and cryptologist from the Brazilian Navy, William Augusto Rodrigues de Souza from DR WARS Laboratories [13] and Anderson C. A. Nascimento from VISA [14] for their availability to provide relevant technical discussions and important observations in corrections to this research.

An Oblivious Transfer(OT) protocol

OT is a protocol in which a sender transfers one of many pieces of information to a receiver but remains oblivious as to what piece has been transferred. The original notion of OT was first proposed by Michael Rabin in 1981 [1] in which a sender sends an encrypted message to a receiver and this one could decrypt such message with probability 1/2. After this, [4] presented a general form of OT, named 1-out-of-2 OT, $\binom{2}{1} - OT$ for short, i.e., where a sender sends two encrypted messages to a receiver being able to decrypt only one of them. Some authors have generalized this to $\binom{n}{1} - OT$ where the receiver chooses one message out of n and $\binom{k}{n} - OT$ in which the receiver chooses a subset of size k from among n messages. In this paper, it will only be considered, $\binom{2}{1} - OT$.

A.1 Protocol $\binom{2}{1} - OT$ Chou-Orlandi

Now, a simplified OT scheme proposed in [14] that inspired the SIOT protocol will be shown as follows.

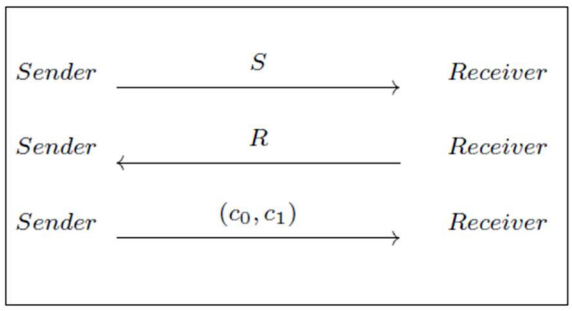
Premises

1. This scheme works in a primitive additive group $(G, B, F_p, +)$ of prime order p, generated by base point B.

2. Let s be a safety parameter and $J \in \{0,1\}$. Thus, the hash function $H : (G \times G) \times G \rightarrow \{0,1\}^s$ is used to generate a cryptographic key k_J for use in a symmetric cipher defined from the functions $\mathcal{E}$ (Encryption) and $\mathcal{D}$ (Decryption), i.e., $c_0 = \mathcal{E}(k_0, m_0)$ and $c_1 = \mathcal{E}(k_1, m_1)$.

3. Abstract view of information exchange from protocol $\binom{2}{1} - OT$ Chou-Orlandi.

[12] https://www.marinha.mil.br/casnav/
[13] https://drwarslabs.com/index.html
[14] https://usa.visa.com/about-visa/visa-research/anderson-nascimento.html



Sender and Receiver

Setup - Sender

1. Sender secretly chooses a value $y \in F_p$;

2. Sender computes:

$$S = y \cdot B \quad (1)$$

$$T = y \cdot S; \quad (2)$$

3. Sender sends S to Receiver which refuses if $S \notin G$.

Setup - Receiver

1. Receiver secretly chooses a value $x \in F_p$;

2. Receiver computes:

$R = b \cdot S + x \cdot B$ (3), where $b \in \{0,1\}$ is chosen by Receiver.

3.Receiver sends R to Sender which refuses if $R \notin G$.

Generation of cryptographic keys $k_J, J \in \{0,1\}$.

1. Sender computes:

$$k_J = H(S,R)(y \cdot R - J \cdot T) \quad (4)$$

2. Receiver computes:

$$k_b = H(S,R)(b \cdot S + x \cdot B) \quad (5)$$

Encryption and Decryption

1. Sender encrypts and sends c = (c_0, c_1) to Receiver. Recalling $c_0 = \mathcal{E}(k_0, m_0)$ and $c_1 = \mathcal{E}(k_1, m_1)$;
2. Receiver decrypts and gets $M_b = \mathcal{D}(k_b, c_J), J \in \{0,1\}$.

Remark 11. It is verified that a key $k_J, J \in \{0,1\}$, is computed by $H(S,R)[x \cdot y \cdot B + (b - J)T]$. Hence, at the end of the protocol if both parts are honest then we have that $k_b = k_J$. In other words, if $J = 0$ then $c = c_0 = 0$ and $k_0 = k_b = H(S,R)(x \cdot y \cdot B)$. Otherwise, if $J = 1$ then $c = c_1 = 1$ and $k_1 = k_b = H(S,R)(x \cdot y \cdot B)$.

$k_J = y \cdot R - J \cdot T$;
$= y(b \cdot S + x \cdot B) - J \cdot T$; from equation (3)
$= b \cdot y \cdot S + x \cdot y \cdot B - J \cdot T$;
$= b \cdot T + x \cdot y \cdot B - J \cdot T$; from equations (1) and (2)
$= x \cdot y \cdot B + (b - J) \cdot T$.

Therefore, it follows that if the Receiver chooses $b \notin J$ and he will not share the secret (cryptographic key) with the Sender. The relative simplicity of this scheme inspired our paper.

A.2 Privacy in an $\binom{2}{1} - OT$ protocol

Now, a privacy definition for an $\binom{2}{1} - OT$ protocol presented in [62] will be seen as follows. Thus, there is an $\binom{2}{1} - OT$ protocol with Sender (S) and Receiver (R). $\Omega_S\{S(1^n, m), R(1^n, z)\}$ denotes the view of S in an execution where it has input m and R has input z and the security parameter is n. Similarly, It is denoted the view of R by $\Omega_R\{S(1^n, m), R(1^n, z)\}$.

Definition 1. (Privacy $\binom{2}{1} -$ *Oblivious Transfer* (OT))
A two-message two-party probabilistic polynomial-time protocol, i.e., S and R, is said to be a private $\binom{2}{1} - OT$ if the following holds:
- ***Non-triviality***: If S and R follow the protocol then, after an execution in which S has for input any pair messages $m_0, m_1 \in \{0,1\}^*$, and R has for input any bit $\sigma \in \{0,1\}$, the output of R is m_σ.
-Privacy in the case of a malicious Sender ($\hat{S}$): For every non-uniform probabilistic polynomial-time $\hat{S}$ and every auxiliary input $m \in \{0,1\}^*$ then,

$$\Omega_{\hat{S}}\{\hat{S}(1^n, m), R(1^n, 0)\}_{n \in \mathbb{N}} \equiv$$
$$\Omega_{\hat{S}}\{\hat{S}(1^n, m), R(1^n, 1)\}_{n \in \mathbb{N}}$$

-Privacy in the case of a malicious Receiver ($\hat{R}$): For every non-uniform deterministic polynomial-time $\hat{R}$, every auxiliary input $z \in \{0,1\}^*$, and every triple of inputs $m_0, m_1, m_2 \in \{0,1\}^*$ such that $|m_0| = |m_1| = |m_2|$ it holds that either:

$$\Omega_{\hat{R}}\{S(1^n, (m_0, m_1)); \hat{R}(1^n, z)\}_{n \in \mathbb{N}} \equiv \Omega_{\hat{R}}\{S((1^n, (m_0, m_2)); \hat{R}(1^n, z)\}_{n \in \mathbb{N}}$$
or
$$\Omega_{\hat{R}}\{S(1^n, (m_0, m_1)); \hat{R}(1^n, z)\}_{n \in \mathbb{N}} \equiv \Omega_{\hat{R}}\{S((1^n, (m_2, m_1)); \hat{R}(1^n, z)\}_{n \in \mathbb{N}}$$

A.2.1 Analyzing the definition of Privacy

Non-Triviality.

The *non-triviality* condition is also called completeness or functionality according to [70]. Then, the Oblivious Transfer functionality is defined by $((m_0, m_1), \sigma) \rightarrow (m_\sigma)$ for some $\sigma \in \{0,1\}$.

Privacy in the case of a malicious Sender.

According to the above definition in the case of $\hat{S}$, for all $\sigma \in \{0,1\}$, denote $R(1^n, \sigma)$ the message sent from the honest R with input $(1^n, \sigma)$. Hence, the ensembles $\{R(1^n,0)\}_{n\in\mathbb{N}}$ and $\{R(1n,1)\}_{n\in\mathbb{N}}$ are computationally indistinguishable to $\hat{S}$, i.e., $\{R(1^n,0)\}_{n\in\mathbb{N}} \equiv \{R(1^n,1)\}_{n\in\mathbb{N}}$. Therefore, this implies that $\hat{S}$ cannot find anything about R's inputs.

Privacy in the case of a malicious Receiver.

In the case of an $\hat{R}$, denote $\hat{R}(1^n, z)$ the first message by $\hat{R}$ and it determines whether it should receive m_0 or m_1 from S. For instance, if it determines that $\hat{R}$ should receive m_0, then both inputs (m_0, m_1) and (m_0, m_2) are indistinguishable to $\hat{R}$. Therefore, this implies that $\hat{R}$ cannot learn anything about m_1 when it receives m_0 and vice versa.

Discussion.

It should be noted that Definition 1 is based on indistinguishability. According to [62], when a party is not supposed to learn anything (i.e. when it has no output), it is easy to define privacy via indistinguishability as for encryption. On the other hand, [70] states that this type of definition, although it is a meaningful and sufficient notion for some applications, is still weaker than the simulation-based notion and, in particular, cannot offer the same composability properties and then, it is more difficult to use it as a building block in secure multi-part computing protocols. Therefore, even with certain limitations, the aforementioned Definition of Privacy based on indistinguishability was adapted with other concepts, i.e., isogenies of elliptic curves to design the security proof of the $\binom{2}{1}$-SIOT protocol with regard to privacy between two parties.

Remark 12. It should be noted that this definition considers the adversarial behavior in OT protocol as malicious. However, in the $\binom{2}{1}$-SIOT protocol, the behavior is considered semi-honest because both S and R even corrupted parties correctly follow the protocol specification.

B Isogenies

In short, isogeny-based cryptography utilizes unique algebraic maps between elliptic curves that satisfy group homomorphism. This original idea introduced by [71] detailed a Diffie-Hellman cryptosystem based on the hardness of computing isogenies between ordinary elliptic curves. Nevertheless, [72] developed a quantum algorithm that could compute isogenies between ordinary curves in subexponential time. This algorithm uses the fact that the structure of the elliptical group is commutative. Thus, [40] adapted the isogeny-based key exchange protocol to be based on the difficulty of computing isogenies between supersingular elliptic curves, which does not have commutative endomorphism ring.

Definition 2. Let E_1 and E_2 be elliptic curves over $\mathbb{F}_p$. An isogeny over $\mathbb{F}_p$ is a morphism $\phi: E_1 \to E_2$ over $\mathbb{F}_p$ such that $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$ is a group homomorphism. The zero isogeny is the constant map $\phi: E_1 \to E_2$ given by $\phi(P) = \mathcal{O}_{E_2}$ for all $P \in E(\overline{\mathbb{F}}_p)$. If there is an isogeny between two elliptic curves E_1 and E_2 then:

i. E_1 and E_2 are isogenous.

ii. $\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p)$[15].

iii. E_1 and E_2 have the same j − invariant if and only if $E_1 \simeq E_2$ over $\overline{\mathbb{F}}_p$ (i.e. exist an isomorphism from E_1 to E_2)[16].

Definition 3. Let E_1 and E_2 be elliptic curves over $\mathbb{F}_p$ and $\phi: E_1 \to E_2$ over $\mathbb{F}_p$. The degree of a non-zero isogeny is the degree of the morphism. The degree of the zero isogeny is 0. If there is an isogeny of degree ℓ between elliptic curves E_1 and E_2 then, they are ℓ-isogenous.

Definition 4. Let E_1 and E_2 be elliptic curves over $\mathbb{F}_p$ and $\phi: E_1 \to E_2$ an isogeny. Then, the kernel of an isogeny is $ker(\phi) = \{P \in E_1(\overline{\mathbb{F}}_p): \phi(P) = \mathcal{O}_{E_2}\}$.

Remark 13. We can denote $E_2 = E_1/ker(\phi)$.

Definition 5. A non-zero isogeny separable $\phi: E_1 \to E_2$ over $\mathbb{F}_p$ of ℓ - degree has $\#ker(\phi) = \ell$.

Definition 6. Let $\phi: E_1 \to E_2$ and $\hat{\phi}: E_2 \to E_3$ be two isogenies with ℓ -degree and $\hat{\ell}$ -degree, respectively. Then, their composition is an isogeny $\hat{\phi}(\phi): E_1 \to E_3$ with $(\ell \cdot \hat{\ell})$-degree.

Proposition 3. Let E_1 be an elliptic curve over $\mathbb{F}_p$ and $\mathbb{G}$ a finite subgroup of $E_1(\overline{\mathbb{F}}_p)$ that is defined over $\mathbb{F}_p$. Then, there is a unique elliptic curve $E_{\mathbb{G}}$ and a separable isogeny $\phi: E_1 \to E_{\mathbb{G}} = E_1/\mathbb{G}$ such that $ker(\phi) = \mathbb{G}$.

Proof See Theorem 25.1.6 and Corollary 25.1.7 from [74].

[15] See [73].

[16] See Theorem 9.3.6 from [74].

C M-SIDH protocol

Figure 5 shows the M-SIDH protocol. Recalling that the Castryck-Decru attack [39] requires two main aspects:
1. The degrees A and B from the secret supersingular isogenies $\phi_A : E_0 \rightarrow E_A$ and $\phi_B : E_0 \rightarrow E_B$, respectively.
2. The images $\phi_A(P_B)$, $\phi_A(Q_B)$ from $\langle P_B, Q_B \rangle =: E_0[B]$, i.e., points of the B-torsion : $E_0[B]$, where B is an integer coprime A such that B > A. Similarly, $\phi_B(P_A)$, $\phi_B(Q_A)$ from $\langle P_A, Q_A \rangle = E_0[A]$, i.e., points of the A torsion $E_0[A]$.

According to the aspects above, [57] suggest masking the torsion point images by random uniform integers, i.e., a multiplication by scalars from $\eta \in \mathbb{Z}/B\mathbb{Z}$ and $\rho \in \mathbb{Z}/A\mathbb{Z}$. Hence, the public keys $(E_A, \phi_A(P_B), \phi_A(Q_B))$ and $(E_B, \phi_B(P_A), \phi_B(Q_A))$ will be changed to $pk_A \leftarrow (E_A, [\eta]\phi_A(P_B), [\eta]\phi_A(Q_B))$ and $pk_B \leftarrow (E_B, [\rho]\phi_B(P_A), [\rho]\phi_B(Q_A))$. On the other hand, one tries to compute the Weil paring values $e_B([\eta]\phi_A(P_B), [\eta]\phi_A(Q_B))$ and $e_A([\rho]\phi_B(P_A), [\rho]\phi_B(Q_A))$, then

$$e_B([\eta]\phi_A(P_B), [\eta]\phi_A(Q_B)) = e_B(P_B, Q_B) = e_B(G_A, H_A)$$
$$= e_B(P_B, Q_B)^{\eta^2 deg\phi_A} = e_B(P_B, Q_B)^{\eta^2 A} e_B(P_B, Q_B)^A.$$

Remark 14. We denote $deg\phi_A = A$. Furthermore, $\eta^2 = 1 \, mod A$. It is worth mentioning that one can sample η from $\mu(B)$ where,

$$\mu(B) = \{\eta \in \mathbb{Z}/B\mathbb{Z} \mid \eta^2 = 1 \, mod \, B\}.$$

It is important to highlight the adversary should not be able to recover the scalar η. Hence, it is necessary an exponential number of square roots of $1 = mod B$. Let λ be a security parameter. Thus, B must have at least λ distinct prime factors such that an exhaustive search of integer η in set of all possible square roots of $\eta^2 mod \, B$ must cost $O(\lambda^2)$. Therefore, $B = \prod_{i=1}^{\lambda} q_i$ where, q_i is small prime. Similarly, the analysis performed on pk_A is valid for pk_B, then

$$e_A([\rho]\phi_B(P_A), [\rho]\phi_B(Q_A)) = e_A(P_A, Q_A) = e_A(G_B, H_B)$$
$$= e_A(P_A, Q_A)^{\rho^2 deg\phi_B} = e_A(P_A, Q_A)^{\rho^2 B} = e_A(P_A, Q_A)^B$$

Furthermore, $\rho^2 = 1 \, mod \, B$ and $deg\phi_B = B$. Finally, one can sample ρ from $\mu(B)$ where,

$$\mu(A) = \{\rho \in \mathbb{Z}/B\mathbb{Z} \mid \rho^2 = 1 \, mod \, A\},$$

Therefore, $A = \prod_{i=1}^{\lambda} \ell_i$, where, ℓ_i is a small prime.

C.1 Public parameters

Let λ be the security parameter and let $t = t(\lambda) \in \mathbb{N}$ be an integer depending on λ. Let E_0 be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. For convenience, assume a prime p of form $p = A \cdot B \cdot f \pm 1$ where both A and B are coprimes integers and $A \approx B \approx \sqrt{p}$. Hence, this choice yields $p = 3(mod\ 4)$, enabling the representation[17] $\mathbb{F}_{p2} = \mathbb{F}_{p[x]}/\langle x^2 + 1 \rangle$. The curve $E_0[\mathbb{F}_{p2}]$ is a randomly generated supersingular initial curve[18] with ring of unknown endomorphism and group order with group order $(A \cdot B \cdot f)^2$. Set $E_0[A]$ and $E_0[B]$ generated by kernel $\langle P_A, Q_A \rangle$ and $\langle P_B, Q_B \rangle$, respectively. The public parameters are $E_0, p, A, B, P_A, Q_A, P_B, Q_B$.

C.2 Generation of key pairs

Setup - Sender

1. Alice chooses randomly and secretly two integers $r_A \leftarrow \$ \, \mathbb{Z}/A\mathbb{Z}$ and $\eta \leftarrow \$ \, \mu(B)$.
2. She computes:
(a) $ker(\phi_A) = \langle P_A + r_A Q_A \rangle$;
(b) $\phi_A : E_0 \rightarrow E_A$;
(c) $G_A \leftarrow [\eta]\phi_A(P_B)$; $H_A \leftarrow [\eta]\phi_A(Q_B)$;
(d) η is deleted.
3. Alice creates a pair of keys $sk_A = (\phi_A, r_A)$ and $pk_A = (E_A, G_A, H_A)$, i.e, her private and public keys, respectively.
4. She sends pk_A to Bob. Then, he checks if $G_A, H_A \in E_A[B]$ and $e_B(G_A, H_A) = e_B(P_B, Q_B)^A$. Otherwise, pk_A will be rejected ($\perp$) and the protocol is restarted.

Remark 15. It is denoted $E_A \cong E_0/\langle P_A + r_A Q_A \rangle$, where $|ker(\phi_A)| = |\langle P_A + r_A Q_A \rangle| = A$,i.e., a separable[19] isogeny of degree A.

Setup - Receiver

1. Bob chooses randomly and secretly two integers $r_B \leftarrow \$ \, \mathbb{Z}/B\mathbb{Z}$ and $\rho \leftarrow \$ \, \mu(A)$;
2. He computes:
(a) $ker(\phi_B) = \langle P_B + r_B Q_B \rangle$;
(b) $\phi_B : E_0 \rightarrow E_B \cong E_0/\langle P_B + r_B Q_B \rangle$;
(c) $G_B \leftarrow [\rho]\phi_B(P_A)$; $HB \leftarrow [\rho]\phi_B(Q_A)$;
(d) ρ is deleted.

[17] See [67] for more details about this type of representation.
[18] Multiparty computation (MPC) techniques generate a random supersingular initial E0 curve with a ring of unknown endomorphism. For more details, see [65].
[19] See [69], Proposition 12.8.

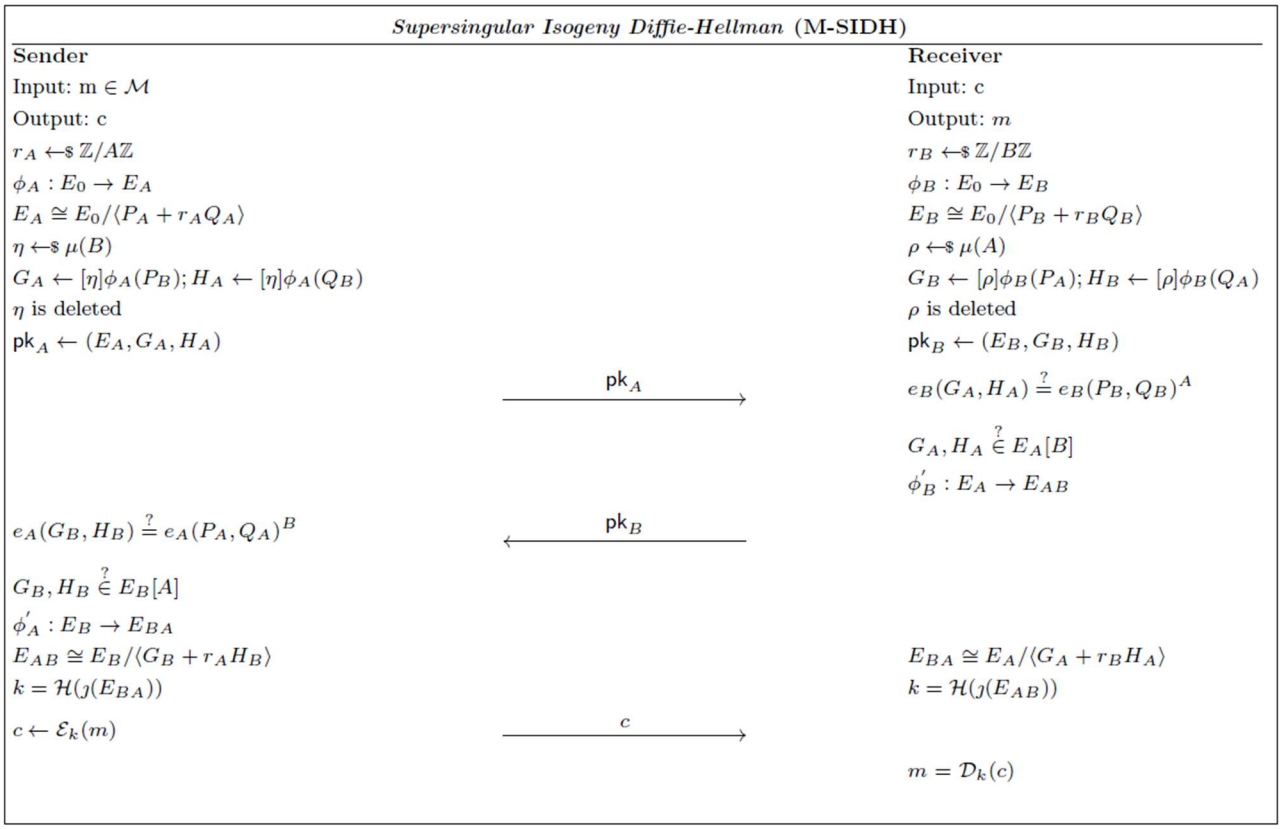


Figure 5: M-SIDH protocol

3. Bob creates a key pair $sk_B = (\phi_B, r_B)$ and $pk_B = (E_B, G_B, H_B)$, i.e., his private and public key, respectively.
4. He sends pk_B to Alice. Then, she checks if $G_B, H_B \in E_B[A]$ and $e_A(G_B, H_B) = e_A(P_A, Q_A)^B$. Otherwise, pk_B will be rejected ($\perp$) and the protocol is restarted.

C.3 Generation of secret keys

Setup – Sender

1. Alice computes:
(a) $ker(\phi'_A) = \langle (G_B + r_A H_B \rangle$.
(b) $\phi'_A : E_B \to E_{AB}$.
(c) $j(E_{AB})$.
(d) $k \leftarrow H(j(E_{AB}))$.

Setup – Receiver

1. Bob computes:
(a) $ker(\phi'_B) = \langle G_A + r_B H_A \rangle$.
(b) $\phi'_B : E_B \to E_{BA}$.
(c) $j(E_{BA})$.
(d) $k \leftarrow H(j(E_{BA}))$.

C.4 Encryption and Decryption

Setup - Sender
1. Alice encrypts m. Then, $c \leftarrow E(k, m)$;
2. She sends c to Bob.

Remark 16. Recall that $pk_A = (E_A, G_A, H_A)$, i.e., Alice's public key is computed at the beginning of the execution process.

Setup - Receiver
1. He decrypts and gets $m \leftarrow D(k, c)$.

Declaration of interests

The authors declare that they have no known competing financial interests or personal relationships that could have influenced the work reported in this paper. Furthermore, this paper reflects a recent doctoral thesis by Gláucio Oliveira from the University of São Paulo, Brazil. Paulo Barreto is the advisor of this doctoral thesis and Waldyr Benits is his assistant. Therefore, the only interest of this work is purely academic dissemination.

References

[1] Rabin, Michael O.: How to Exchange Secrets with Oblivious Transfer. http://eprint.iacr.org/2005/187 (2005).

[2] Naor, Moni., Pinkas, Benny., Reuban, Sumner.: EC '99: Proceedings of the 1st ACM conference on Electronic commerce, Pages 129–139, https://doi.org/10.1145/336992.337028 (1999).

[3] Garay, J.A., Jakobsson, M.: Timed Release of Standard Digital Signatures, In Financial Cryptography '02, LNCS 2537, Pages 168-182, Springer-Verlag,https://doi.org/10.1007/3-54036504-4_13 (2002).

[4] Even, S., Goldreich, O., Lempel, A.: A Randomized Protocol for Signing Contracts. Communications of the ACM. 28. 205-210. https://doi:10.1145/3812.3818 (1982).

[5] Lísková, L., Stanek, M.: Efficient Simultaneous Contract Signing. In: Deswarte, Y., Cuppens, F., Jajodia, S., Wang, L. (eds) Security and Protection in Information Processing Systems. SEC 2004. IFIP — The International Federation for Information Processing, vol 147. Springer, Boston, MA. https://doi.org/10.1007/1-4020-8143-X_29 (2004).

[6] Staneková, L., Stanek, M.: Fast Contract Signing with Batch Oblivious Transfer. In: Dittmann, J., Katzenbeisser, S., Uhl, A. (eds) Communications and Multimedia Security. Lecture Notes in Computer Science, vol 3677. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11552055_1 (2005).

[7] Goldreich, O., Micali, S., Wigderson, A.: How to play any mental game. In Proceedings of the nineteenth annual ACM symposium on Theory of computing. Association for Computing Machinery, New York, NY, USA, 218–229. https://doi.org/10.1145/28395.28420 (1987).

[8] Beaver, D.: Minimal-Latency Secure Function Evaluation. In: Prenell, B. (eds) Advances in Cryptology — EUROCRYPT. Lecture Notes in Computer Science, vol 1807. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45539-6_23 (2000).

[9] Bellare, Mihir., Micali, Silvio.: Non-Interactive Oblivious Transfer and Applications. In: Brassard, G. (eds) Advances in Cryptology — CRYPTO Proceedings. Lecture Notes in Computer Science, vol 435. Springer, New York, NY. https://doi.org/10.1007/0-387-34805-0_48 (1990).

[10] Naor, Moni., Pinkas, Benny.: Efficient oblivious transfer protocols. In Proceedings of the twelfth annual ACMSIAM symposium on Discrete algorithms. Society for Industrial and Applied Mathematics, USA, 448–457. https://dl.acm.org/doi/10.5555/365411.365502 (2001).

[11] Aiello, William., Ishai, Yuval., Reingold, Omer.: Priced Oblivious Transfer: How to Sell Digital Goods. In: Pfitzmann, B. (eds) Advances in Cryptology — EUROCRYPT. Lecture Notes in Computer Science, vol 2045. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-44987-6_8 (2001).

[12] Wu, Q.-H., Zhang, J.-H., and Wang, Y.-M.: Practical t out-n Oblivious Transfer and Its Applications. In: Qing, S., Gollmann, D., Zhou, J. (eds) Information and Communications Security. ICICS. Lecture Notes in Computer Science, vol 2836. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-39927-8_21 (2003).

[13] Zhang, Bingsheng., Lipmaa, Helger., Wang, Cong., Ren, Kui.: Practical Fully Simulatable Oblivious Transfer with Sublinear Communication. In: Sadeghi, AR. (eds) Financial Cryptography and Data Security. Lecture Notes in Computer Science, vol 7859. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-39884-1_8 (2013).

[14] Chou, Tung., Orlandi, Claudio.: The Simplest Protocol for Oblivious Transfer. In: Lauter, K., Rodríguez-Henríquez, F. (eds) Progress in Cryptology– LATINCRYPT. Lecture Notes in Computer Science (), vol 9230. Springer, Cham. https://doi.org/10.1007/978-3-319-22174-8_3 (2015).

[15] Shor, Peter W.: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM J. Comput. 26, 5 (Oct. 1997), 1484–1509. https://doi.org/10.1137/S0097539795293172 (1997).

[16] National Institute of Standards and Technology (NIST).: Report on Post-Quantum Cryptography. http://dx.doi.org/10.6028/NIST.IR.8105 (2016).

[17] Crépeau, Claude., Kilian, J.: Achieving oblivious transfer using weakened security assumptions. In Proceedings of the 29th Annual Symposium on Foundations of Computer Science (SFCS). IEEE Computer Society, USA, 42–52. https://doi.org/10.1109/SFCS.1988.21920 (1988).

[18] Bennett, Charles H., Brassard, Gilles., Crépeau, Claude., Skubiszewska, Marie-Helene.: Practical Quantum Oblivious Transfer. In: Feigenbaum, J. (eds) Advances in Cryptology— CRYPTO '91. Lecture Notes in Computer Science, vol 576. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-46766-1_29 (1991).

[19] Mayers, D., Salvail. L.: Quantum Oblivious Transfer is secure against all individual measurements. Physics and Computation, 1994. Phys Comp'94, Pages:69,70,71,72,73,74,75,76,77, https://doi.ieeecomputersociety.org/10.1109/PHYCMP.1994.363696 (1994).

[20] Yao, A.: Security of quantum protocols against coherent measurements. In Proceedings of the twenty-seventh annual ACM symposium on Theory of computing (STO'95). Association for Computing Machinery, New York, NY, USA, 67 – 75. https://doi.org/10.1145/225058.225085 (1995).

[21] Mayers, D.: Quantum Key Distribution and String Oblivious Transfer in Noisy Channels. In: Koblitz, N. (eds) Advances in Cryptology— CRYPTO'96. Lecture Notes in Computer Science,

vol 1109. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-68697-5_26 (1996).
[22] Damgard, Ivan., Fehr, Serge., Lunemann, Carolin., Salvail, Louis., Schaffner, Christian.: Improving the Security of Quantum Protocols via Commit-and-Open. In: Halevi, S. (eds) Advances in Cryptology - CRYPTO 2009. Lecture Notes in Computer Science, vol 5677. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-03356-8_24 (2009).
[23] Unruh, D.: Universally Composable Quantum Multiparty Computation. In: Gilbert, H. (eds) Advances in Cryptology–EUROCRYPT 2010. Lecture Notes in Computer Science, vol 6110. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-13190-5_25 (2010).
[24] Dowsley, Rafael., van de Graaf, Jeroen., Muller-Quade, Jörn., Nascimento, Anderson C. A.: Oblivious Transfer Based on the McEliece Assumptions. In: Safavi-Naini, R. (eds) Information Theoretic Security. ICITS 2008. Lecture Notes in Computer Science, vol 5155. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-850 93 -9_11 (2008).
[25] David, Bernardo., Nascimento, C. A. Anderson., Muller-Quade, Jörn.: Universally Composable Oblivious Transfer from Lossy Encryption and the McEliece Assumptions. In: Smith, A. (eds) Information Theoretic Security. ICITS 2012. Lecture Notes in Computer Science, vol 7412. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-32284-6_5 (2012).
[26] David, Bernardo., Dowsley, Rafael., Nascimento, C.A.: Universally Composable Oblivious Transfer Based on a Variant of LPN. In: Gritzalis, D., Kiayias, A., Askoxylakis, I. (eds) Cryptology and Network Security. CANS 2014. Lecture Notes in Computer Science, vol 8813. Springer, Cham. https://doi.org/10.1007/978-3-319-12280-9_10
[27] S. L. M. Barreto, Paulo., David, Bernardo., Dowsley, Rafael., Mozorov, Kirill., C. A. Nascimento, Anderson.: A framework for efficient adaptively secure composable oblivious transfer in the ROM. Cryptology ePrint Archive, https://eprint.iacr.org/2017/993 (2017).
[28] Dottling, Nico., Garg, Sanjam., Hajiabadi, Mohammad., Masny, Daniel., Wichs, Daniel.: Two-Round Oblivious Transfer from CDH or LPN. In: Canteaut, A., Ishai, Y. (eds) Advances in Cryptology – EUROCRYPT 2020. Lecture Notes in Computer Science, vol 12106. Springer, Cham. https:// doi.org/ 10.1007/978-3-030-45724-2_26 (2020).
[29] Peikert, Chris., Vaikuntanathan, Vinod., Waters, Brent.: A Framework for Efficient and Composable Oblivious Transfer. In David Wagner, editor, Advances in Cryptology - CRYPTO 2008, volume 5157 of Lecture Notes in Computer Science, pages 554-571, Santa Barbara, CA, USA, August 17-21, 2008. Springer, Heidelberg, Germany. https://link.springer.com/content/pdf/10.1007/978-3-540-85174-5_31.pdf (2008).
[30] Kazmi, R.: Cryptography from Post-Quantum Assumptions. Cryptology ePrint Archive, http://eprint. iacr.org/2015/376 (2015).
[31] Brakerski, Zvika., D¨ottling, Nico.: Two-Message Statistically Sender-Private OT from LWE. In: Beimel, A., Dziembowski, S. (eds) Theory of Cryptography. TCC 2018. Lecture Notes in Computer Science, vol 11240. Springer, Cham. https://doi.org/10.1007/978-3-030-03810-6_14 .
[32] Micciancio, Daniele., Sorrell, Jessica.: Simpler Statistically Sender Private Oblivious Transfer from Ideals of Cyclotomic Integers. In: Moriai, S., Wang, H. (eds) Advances in Cryptology – ASIACRYPT 2020. Lecture Notes in Computer Science, vol 12492. Springer, Cham. https://doi.org/10.1007/978-3-030-64834-3_13 (2020).
[33] Vitse, Vanessa.: Simple oblivious transfer protocols compatible with Kummer and supersingular isogenies. Archives-Ouvertes. https://hal.science/hal-01981552/document (2019).
[34] Branco P., Ding J., Goulão M., Mateus P.: A framework for composable oblivious transfer from one-round key exchange. Em Albrecht M., editor, Cryptography and Coding. IMACC 2019. Lecture Notes in Computer Science, volume 11929. Springer. https://link.springer.com/book/10.1007/978-3-030-35199-1 (2019).
[35] de Saint Guilhem, Cyprien., Orsini, Emmanuela., Petit, Christophe., P. Smart, Nigel.: Semi-commutative Masking: A Framework for Isogeny-Based Protocols, with an application to Fully Secure Two-Round Isogeny-Based OT. In: Krenn, S., Shulman, H., Vaudenay, S. (eds) Cryptology and Network Security. CANS 2020. Lecture Notes in Computer Science, vol 12579. Springer, Cham. https://doi.org/10.1007/978-3-030-65411-5_12
[36] Lai, Yi-Fu., Galbraith, Steven D., de Saint Guilhem, Cyprien.: Compact, Efficient and UC-Secure Isogeny-Based Oblivious Transfer. In: Canteaut, A., Standaert, FX. (eds) Advances in Cryptology – EUROCRYPT 2021. Lecture Notes in Computer Science, vol 12696. Springer, Cham. https://doi.org/10.1007/978-3-030-77870-5_8 (2021).
[37] Maino, L., Martindale, C.: An attack on SIDH with an arbitrary starting curve. Cryptology ePrint Archive, https://eprint.iacr.org/2022/1026 (2022).
[38] Robert, Damien.: Breaking SIDH in Polynomial Time. Cryptology ePrint Archive. https://eprint. iacr.org/2022/1038 (2022).
[39] Castryck, W., Decru, T.: An Efficient Key Recovery Attack on SIDH. In: Hazay, C., Stam, M. (eds) Advances in Cryptology – EUROCRYPT 2023. Lecture Notes in Computer Science, vol 14008. Springer, Cham. https://doi.org/10.1007/978-3-031-30589-4_15 (2023).
40. De Feo, L., Jao, D., Plut, J.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Journal of Mathematical Cryptology,

8(3), 209-247. https://doi.org/10.1515/jmc-2012-0015 (2014).
[41] Azarderakhsh, Reza., Campagna, Matthew., Costello, Craig., Feo, LD., Hess, Basil., Jalali, A., Jao, D., Koziel, B., LaMacchia, B., Longa, P., et al.: Supersingular Isogeny Key Encapsulation (SIKE). https://sike.org (2017).
[42] Charles, D.X., Lauter, K.E. & Goren, E.Z.: Cryptographic Hash Functions from Expander Graphs. J Cryptol 22, 93–113. https://doi.org/10.1007/s00145-007-9002-x (2009).
[43] Castryck, Wouter., Lange, Tanja., Martindale, Chloe., Panny, Lorenz., Renes, Joost.: CSIDH: An Efficient Post-Quantum Commutative Group Action. In Advances in Cryptology – ASIACRYPT 2018: 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2–6, 2018, Proceedings, Part III. Springer-Verlag, Berlin, Heidelberg, 395–427. https://doi.org/10.1007/978-3-030-03332-3_15 (2018).
[44] Beullens, Ward., Kleinjung, Thorsten., Vercauteren, Frederik.: CSI-FiSh: Efficient Isogeny Based Signatures Through Class Group Computations. In: Galbraith, S., Moriai, S. (eds) Advances in Cryptology – ASIACRYPT 2019. Lecture Notes in Computer Science, vol 11921. Springer, Cham. https://doi.org/10.1007/978-3-030-34578-5_9 (2019).
[45] De Feo, Luca., Galbraith, Steven D.: SeaSign: Compact Isogeny Signatures from Class Group Actions. In: Ishai, Y., Rijmen, V. (eds) Advances in Cryptology – EUROCRYPT 2019. Lecture Notes in Computer Science, vol 11478. Springer, Cham. https://doi.org/10.1007/978-3-030-17659-4_26.
[46] De Feo, Luca., Kohel, David., Leroux, Antonin., Petit, Christophe., Wesolowski, Benjamin.: SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies. In: Moriai, S., Wang, H. (eds) Advances in Cryptology– ASIACRYPT 2020. Lecture Notes in Computer Science, vol 12491. Springer, Cham. https://doi.org/10.1007/978-3-030-64837-4_3 (2020).
[47] Galbraith, S.D., Petit, C., Silva, J.: Identification Protocols and Signature Schemes Based on Supersingular Isogeny Problems. J Cryptol 33, 130–175. https://doi.org/10.1007/s00145-019-09316-0 (2020).
[48] Branco, Pedro., Ding, Jintai., Goulão, Manuel., Mateus, Paulo.: Universally Composable Oblivious Transfer Protocol based on the RLWE Assumption. Cryptology ePrint Archive. https://eprint.iacr.org/2018/1155.pdf (2018).
[49] Valencia, F R.: Genus 2 Supersingular Isogeny Oblivious Transfer. https://arxiv.org/abs/1907.0045 (2019).
[50] De Feo, Luca.: Tools for designing protocols based on isogenies Bristol, UK (virtual). Lecture notes for the Isogeny based cryptography school 2020. https://defeo.lu/docet/assets/misc/2021-08-02-isogeny-school.pdf.
[51] Kundu, N., Debnath, S.K., Mishra, D.: 1-out-of-2: post quantum oblivious transfer protocols based on multivariate public key cryptography. Sādhanā 45, 209. https://doi.org/10.1007/s12046-020-01447-6 (2020).
[52] Boneh, D., Kogan, D., Woo, K.: Oblivious Pseudorandom Functions from Isogenies. In: Moriai, S., Wang, H. (eds) Advances in Cryptology – ASIACRYPT 2020. Lecture Notes in Computer Science, vol 12492. Springer, Cham. https://doi.org/10.1007/978-3-030-64834-3_18.
[53] Alamati, N., De Feo, L., Montgomery, H., Patranabis, S.: Cryptographic Group Actions and Applications. In: Moriai, S., Wang, H. (eds) Advances in Cryptology – ASIACRYPT 2020. Lecture Notes in Computer Science, vol 12492. Springer, Cham. https://doi.org/10.1007/978-3-030-64834-3_14 (2020).
[54] Leroux, A.: A New Isogeny Representation and Applications to Cryptography. In: Agrawal, S., Lin, D. (eds) Advances in Cryptology – ASIACRYPT 2022. Lecture Notes in Computer Science, vol 13792. Springer, Cham. https://doi.org/10.1007/978-3-031-22966-4_1 (2022).
[55] Orsini, E., Zanotto, R.: Simple Two-Round OT in the Explicit Isogeny Model. Cryptology ePrint Archive, https://eprint.iacr.org/2023/269.pdf (2023).
[56] Badrinarayanan, S., Masny, D., Mukherjee, P., Patranabis, S., Raghuraman, S., Sarkar, P.: Round-Optimal Oblivious Transfer and MPC from Computational CSIDH. In: Boldyreva, A., Kolesnikov, V. (eds) Public-Key Cryptography–PKC 2023. Lecture Notes in Computer Science, vol 13940. Springer, Cham. https://doi.org/10.1007/978-3-031-31368-4_14 (2023).
[57] Fouotsa, T.B., Moriya, T., Petit, C.: M-SIDH and MD-SIDH: Countering SIDH Attacks by Masking Information. In: Hazay, C., Stam, M. (eds) Advances in Cryptology–EUROCRYPT 2023. Lecture Notes in Computer Science, vol 14008. Springer, Cham. https: //doi.org/10.1007/978-3-031-30589-4_10 (2023).
[58] Castrick, W., Vercauteren, F.: A polynomial time attack on instances of M-SIDH and FESTA. Cryptology ePrint Archive, https://eprint.iacr.org/2023/1433.pdf (2023).
[59] Galbraith, S.: New cryptanalysis of M-SIDH isogeny cryptography. https://ellipticnews.wordpress.com (2023).
[60] Costello, Craig.: The Case for SIKE: A Decade of the Supersingular Isogeny Problem. Cryptology ePrint Archive, Paper 2021/543.https://eprint.iacr.org/2021/543 (2021).
[61] Barreto, P., Nascimento, A., Oliveira, G., Benits, W.: Supersingular Isogeny Oblivious Transfer (SIOT). Cryptology ePrint Archive, Report 2018/459. https://eprint.iacr.org/2018/459 (2018).

[62] Hazay, C., Lindell, Y.: Efficient Secure Two – Party Protocols - Techniques and Constructions. Springer Berlin Heidelberg. https://link.springer.com /book/10.1007/978-3-642-14303-8 (2010).
[63] Flynn E.V., Ti Y.B.: Genus two isogeny oblivious cryptography. In Post-Quantum Cryptography. Lecture Notes in Computer Science, Springer, volume 11505. 10th International Conference. https://link.springer.com/10.1007/978-3-030-25510-7 (2019).
[64] Petit, Christophe.: Faster Algorithms for Isogeny Problems Using Torsion Point Images. In: Takagi, T., Peyrin, T. (eds) Advances in Cryptology – ASIACRYPT 2017. Lecture Notes in Computer Science, vol 10625. Springer, Cham. https://doi.org/ 10.1007/978-3-319-70697-9_12.
[65] Basso, A., Codogni, G., Connolly, D., De Feo, L., Boris Fouotsa, T., Maria Lido, G., Morrison, T., Panny, L., Patranabis, S., and Wesolowski, B.: Supersingular curves you can trust. https://eprint.iacr. org/2022/1469. (2022)
[66] Wagner, D.: Technical Perspective: Fairness and the Coin Flip. Communications of the ACM. Volume 59, Issue 4, pp 75, https://doi.org/ 10.1145/2898429 (2016).
[67] Hoffstein, J., Pipher, Jill., Silverman, J H.: An introduction to mathematical cryptography. Undergraduate Texts in Mathematics. Springer New York, NY, https://doi:10.1007/978-1-4939-1711-2 (2014).
[68] Silverman, J H.: The arithmetic of elliptic curves. Graduate Texts in Mathematics. Springer New York, NY, https://doi:10.1007/978-0-387-09494-6 (2009).
[69] Washington, L C.: Elliptic curves - Number Theory and Cryptography. Taylor & Francis Group. LLC. https://doi.org/10.1201/9781420071474 (2008).
[70] Kalai, Y T.: Smooth Projective Hashing and Two-Message Oblivious Transfer. In: Cramer, R. (eds) Advances in Cryptology – EUROCRYPT 2005. Lecture Notes in Computer Science, vol 3494. Springer, Berlin, Heidelberg. https://doi.org/10.1007 /11426639_5 (2005)
71. Stolbunov, A.: Cryptography Schemes based on Isogenies. Cryptology ePrint Archive, Paper 2006/145. https://eprint.iacr.org/2006/145 (2006).
[72] Childs, A M., Jao, D., Soukharev, V.: Constructing elliptic curve isogenies in quantum subexponential time. Journal of Mathematical Cryptology, 8(1), 1-29. https://doi.org/10.1515/jmc-2012-0016 (2014).
[73] Tate, J.: Endomorphisms of abelian varieties over finite fields. Invent Math 2, 134–144. https://doi.org/10.1007/BF01404549 (1996).
74. Galbraith, S D.: Mathematics of public key cryptography. Cambridge University Press, Cambridge. https://doi.org/10.1017/CBO9781139012843 (2012).