Supersingular Isogeny-Based Designated Verifier Blind Signature

Rajeev Anand Sahu[1], Agnese Gini[1] and Ankan Pal[2]

University of Luxembourg[1]
University of L'Aquila[2]

Abstract. Recently, Srinath and Chandrasekaran have proposed an undeniable blind signature scheme (UBSS) from supersingular isogeny to provide signer's control in a quantum-resistant blind signature. However, certain weaknesses of undeniable signature have already been observed and have been overcome by formalizing the designated verifier signature (DVS). In this paper, we explore the possibility of generic construction of a DVS from hard homogeneous spaces. Further, following this motivation, we realize a quantum-resistant designated verifier blind signature (DVBS) scheme based on supersingular isogenies from the proposed generic construction. In contrast to the UBSS, our construction do not require interactive communication between the signer and the verifier, yet engages the signer in the verification. The compact signature adds more security properties in a quantum-resistant blind signature to be useful in specific applications including electronic tendering, online auctions etc.

Keywords: Supersingular elliptic curves, Isogeny, Post-quantum signature, Designated verifier signature, Blind signature.

1 Introduction

At the turn of the century, we are at the verge of a quantum era which would render many cryptographic schemes unsafe. This paradigm shift has called for drastic change in the way we perceive the subject. More precisely, most of the public-key cryptographic protocols whose security are based on hard mathematical problems like integer factorization and discrete logarithm problem (DLP), considering the classical computers, would be vulnerable by large-scale quantum computers, for instance following an algorithm due to Shor [31]. This threat recommends development of quantum-resistant primitives. In less than past two decades, the preparation to address this upcoming risk has taken shape and recognized as a fast growing topic of research referred to as post-quantum cryptography (PQC). Currently in the last 4-5 years this topic has received utmost attention as the National Security Agency (NSA) has announced its plans to shift to quantum-immune algorithms and National Institute of Standards and Technology (NIST) is conducting a project to standardize post-quantum public-key cryptography. Some practical outcomes– like the quantum supremacy achieved recently by Google [1]– also encourage researchers to attain practical quantum-resistant schemes in the soonest possible time. In this line of research, certain candidate constructions

have already been proposed including lattice-based [15,28], code-based [22], multivariate equations-based [25], hash-based [23] and isogeny-based [18]. The last one is comparatively recent and offers primitive with smaller key size. In this paper, we consider constructions based on isogenies over supersingular elliptic curves. In the heart of the isogeny-based cryptography are the *supersingular* elliptic curves. The security of the primitives is based on the difficulty of finding a path in the isogeny graph of supersingular elliptic curves. The known quantum algorithm to solve this problem due to Biasse et al. [2] has exponential time complexity.

Motivated from the approach by Couveignes [9] of integrating the hard homogeneous spaces (HHS) in the class field theory (CFT) to couple the DLP into HHS, Rostovtsev and Stolbunov [29] constructed rational-morphism-based cryptosystems on ordinary curves. These protocols had many security flaws and were not quantum safe. The supersingular isogeny graphs were first considered in the construction of collision-resistant hash function from expander graphs by Charles et al [5]. This was a turning point, as it had the potential for providing a quantum safe platform. In the consequent years, Stolbunov [34] proposed a Diffie-Hellman key exchange (DHKE) utilizing isogenies between ordinary elliptic curves, for which Childs et al. [8] showed recovery of private key in sub-exponential time for quantum case. Another paradigm shift in this regard was through the works of Jao and De Feo [18] who introduced DHKE inspired by [29,34] and using isogenies of supersingular elliptic curves. This lead to the construction of public-key encryption scheme and interactive identification protocol [12] from supersingular isogeny. Though, in his doctoral thesis, Stolbunov [35] outlined a probable idea of digital signature from isogenies, but strong designated verifier signature by Xi et al [36] and undeniable signature of Jao and Soukharev [19] were the initial proposals of concrete signature schemes using the properties of isogenies between supersingular elliptic curves. A generalization of the isogeny-based digital signature schemes, from supersingular elliptic curves, were presented by Galbraith et al. [14] and Yoo et al. [41]. The first signature of [14] and the signature of [41] were obtained applying the Unruh's transformation [38]– a quantum analogue of the Fiat-Shamir transform [13]– on the De Feo-Jao-Plût [12] identification protocol. The signature in [14] achieves space optimization due to smaller size than that of [41].

To achieve off-line anonymity, David Chaum [6] introduced the idea of blind signatures. It is essentially an interactive protocol where a requester receives signature on a message from a signer in a way that the actual message and the actual signature is blinded to the signer. Due to its property of anonymity, this signature finds excellent applications in electronic cash system viz. untraceable payments, and electronic voting system. The main security requirements of blind signature are unforgeability and blindness. Security challenges of blind signature are broadly described in [20,27,30]. The idea of undeniable signature [7] was introduced to provide signer's control in the signature's verification. This is obtained by directly involving the signer in the verification procedure. The signer can decide when a signature has to be verified. Such a signature is useful in application like licensing software etc. Unfortunately, certain fundamental weaknesses [11], blackmailing [16] and man-in-the-middle attack [10] have been observed

for the undeniable signature which marginalize its practical applications. Another obvious roadblock is the requirement that the signer has to be available online always for the verification, which is a less viable deal. To address these observed weaknesses of the undeniable signature, the notion of designated verifier signature (DVS) [17] was proposed. A DVS is issued for an authorized verifier who can only verify the signature but cannot transfer the conviction of verification to any third party.

1.1 Contribution

Recently, Srinath and Chandrasekaran [33] proposed isogeny-based quantum-resistant undeniable blind signature scheme (UBSS) by adding the properties of blind signature into the Jao-Soukharev's quantum-resistant undeniable siganture [19]. The main objective of the construction is to provide control to the signer in the quantum-resistant blind signature. As discussed above, the main motivation of an undeniable signature is to achieve signer's involvement in the verification (without acting maliciously) in order to avoid undesirable verifiers who can be convinced of the validity of the signatures. However, in undeniable signature the signer does not have control over the verifier in the sense that she can recognize the authorized verifier beforehand (i.e. before the interaction). Also, a recent observation by Merz et al. [24] shows the possibility of solving the underlying hard problems of the undeniable signatures [19,33] in polynomial time.

To address the observed weaknesses of undeniable signature in a post-quantum undeniable blind signature, in this paper, we propose a supersingular isogeny-based designated verifier blind signature (SI-DVBS) scheme. A relevant work to our proposal is the paper by Xi et al. [36], which offers a strong designated verifier signature from supersingular isogeny (SI-SDVS). Considering the involvement of (private, public) key pair of signer and verifier respectively in the signing and the (public, private) key pair in verification phase, it is straight forward to obtain SI-SDVS following the SIDH [18]. Further, in [36] the property of strongness– i.e. privacy of signer's identity– provides anonymity to the signer in a sense that when such a signature is trapped even before reaching to the designated verifier, it cannot be distinguished among the possible signers that exactly who has signed the message. In contrast to this approach, we achieve anonymity of signer by the means of blind signature which is a more standard and effective practice of realizing anonymous signature than attaining strongness. Moreover, we provide proof of achieving additional security properties like *unverifiability* for such a signature.

Our motivation to this work is to offer more suitable and practical alternate of the quantum-resistant UBSS, by adding more security properties. Moreover, in the view of [33], we eliminate the undesirable communication between the signer and the verifier and hence overhead due to this interaction. Additionally, we also give an instance where our approach can be generalized to realize a designated verifier signature under different security assumptions including those in classical setup as well. To the best of our knowledge, the only proposal of designated verifier blind signature in the classical platform is [42]. Furthermore, we have not observed any such signature in any post-quantum setting yet.

1.2 Outline of the Paper

The rest of this paper is organized as follows. In Section 2, we introduce some related mathematical notions, definitions and problems. In Section 3 we elaborate the approach of our construction in more generic sense and discuss the possibility of constructing designated verifier signature in general under different assumptions. In Section 4, we formalize definition of the supersingular isogeny-based designated verifier blind signature (SI-DVBS) scheme and discuss the security properties of SI-DVBS scheme. Our proposed SI-DVBS signature scheme is presented in Section 5. We analyse the security of our scheme in Section 6 and lastly present a brief conclusion of our work in Section 7.

2 Background

In this section we introduce the notations used in the paper, some relevant definitions and computational problems. We refer [32,40,18,19] for mathematical notions and definitions related to finite field, elliptic curve and isogenies.

A probabilistic polynomial time (PPT) algorithm is a probabilistic/randomized algorithm that runs in time polynomial in the length of input. We denote by $y \leftarrow A(x)$ the operation of running a randomized or deterministic algorithm A with input x and storing the output to the variable y. If X is a set, then $v \xleftarrow{s} X$ denotes the operation of choosing an element v of X according to the uniform random distribution on X. We say that a given function $f : N \rightarrow [0,1]$ is *negligible in n* if $f(n) < 1/p(n)$ for any polynomial p for sufficiently large n [21].

An elliptic curve is a non-singular projective curve of genus one with a specified base point. For practical application, elliptic curves can be considered as plane non-singular cubics with fixed Weierstrass co-ordinates. These varieties are particularly interesting due to the fact that they can be endowed with a group law, expressed in terms of regular morphisms. It is natural then to consider morphisms of curves which are homomorphisms of groups. Let E_0 and E_1 be elliptic curves defined over field $\mathbb{F}$, an *isogeny* $\phi : E_0 \rightarrow E_1$ is a morphism of curves which is also a homomorphism of groups. In this case, E_0 and E_1 are said to be isogenous. Tate's theorem [37] says that two curves E_0 and E_1 defined over a finite field $\mathbb{F}$ are isogenous if and only if they have the same number of $\mathbb{F}$-rational points, i.e. $\#E_0(\mathbb{F}) = \#E_1(\mathbb{F})$.
Each isogeny $\phi : E_0 \rightarrow E_1$ induces an injection between the fields of rational functions of the curve that fixes $\mathbb{F}$ by map $\phi^* : \mathbb{F}(E_1) \rightarrow \mathbb{F}(E_0)$. The *degree* of ϕ (denoted as $\deg\phi$) is defined as $[\mathbb{F}(E_0) : \phi^*(\mathbb{F}(E_1))]$. In this view, an isogeny is said to be *separable* (inseparable) if the induced field extension is separable (inseparable). An isogeny of degree ℓ is called ℓ-isogeny.

Each separable isogeny can be identified (up to isomorphism) with its kernel (denoted as ker). In particular, if E_0 is an elliptic curve defined over $\mathbb{F}$, and G is a finite subgroup of E_0, then there exists a *unique* separeble isogeny $\phi : E_0 \rightarrow E_1$ defined up to

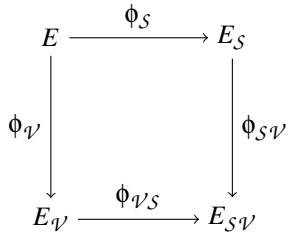
$\overline{\mathbb{F}}$-isomorphism such that $\ker\phi = G$ and $\#\ker\phi = \deg\phi$. The image curve E_1 is defined up to isomorphism and denoted by E_0/G. An explicit representative of a quotient can be determined using Vélu's formulae [39]. Throughout this paper we determine elliptic curves as quotients, thus we always identify each curve with its isomorphism class. Moreover, every class of $\overline{\mathbb{F}}$-isomorphic curves is uniquely identified by an element of $\overline{\mathbb{F}}$, the *j-invariant*. Given an elliptic curve E, its j-invariant $j(E)$ can be computed by the coefficients of a Weierstrass form. Further, the fact that two elliptic curves are isomorphic or not can be verified by just comparing their j-invariants.

If the kernel of an n-isogeny is cyclic then the isogeny is said to be *cyclic* and we say that the two curves are *n-isogenous*. Let E be an elliptic curve defined over $\mathbb{F}$, then for a positive integer n, the *n-torsion subgroup* of E is defined as $E[n] = \{P \in E \mid nP = O\}$, where O is the identity element of E. Given a prime ℓ, co-prime to the characteristic of the base field, the torsion group $E[\ell]$ is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$. Hence E has $\ell+1$ cyclic subgroups of order ℓ and there are (up to isomorphism) exactly $\ell+1$ distinct (separable) isogenies of degree ℓ with domain E.

In the set of supersingular elliptic curves defined over $\overline{\mathbb{F}}$, an *isogeny graph* is a graph whose nodes represent elliptic curves (up to isomorphism) and edges represent isogenies between them. Let E_0 and E_1 be elliptic curves defined over $\mathbb{F}$, then for the isogeny $\phi : E_0 \rightarrow E_1$ of degree n, there exists a unique isogeny $\hat{\phi} : E_1 \rightarrow E_0$, called the *dual* of ϕ, such that $\phi \circ \hat{\phi} = \hat{\phi} \circ \phi = n$, where n is a multiplication map. Hence isogeny graph can be considered undirected.

The set of all endomorphisms of an elliptic curve E, denoted as $End(E)$, forms a ring under the operations of pointwise addition and functional composition. If an elliptic curve E is defined over a field of positive characteristic, then $End(E)$ is isomorphic either to an order in a quaternion algebra or an order in an imaginary quadratic field. In the first case, the elliptic curve is said to be *supersingular* and in the latter *ordinary*. Tate [37] proved that an ordinary and a supersingular curve cannot be isogenus. In particular, it is possible to prove that the supersingular elliptic curves define a connected component of the isogeny graph whose node can be represented using only $j \in \mathbb{F}_{p^2}$. If we restrict to consider only cyclic isogenies of prime degree ℓ, we obtain a $\ell+1$-regular graph. This ℓ-isogeny graph has many good properties, in particular it has been proved to be an expander graph.

In our construction, we consider as base field $\mathbb{F}_{p^2}$ where p is prime of the form $p = \ell_{\mathcal{R}}^{e_{\mathcal{R}}} \ell_{\mathcal{S}}^{e_{\mathcal{S}}} \ell_{\mathcal{V}}^{e_{\mathcal{V}}} \ell_M^{e_M} f \pm 1$ where ℓ_i are distinct small primes, e_i are positive integers and $f \geq 1$ is a small cofactor. We fix a supersingular curve E over $\mathbb{F}_{p^2}$ and $\{P_{\mathcal{R}}, Q_{\mathcal{R}}\}, \{P_{\mathcal{S}}, Q_{\mathcal{S}}\}$, $\{P_{\mathcal{V}}, Q_{\mathcal{V}}\}$ and $\{P_M, Q_M\}$ bases of the $\ell_{\mathcal{R}}^{e_{\mathcal{R}}}, \ell_{\mathcal{S}}^{e_{\mathcal{S}}}, \ell_{\mathcal{V}}^{e_{\mathcal{V}}}$, and $\ell_M^{e_M}$-torsion groups respectively. These public parameters are implicitly provided for all the problems discussed below. For more details of the notations please refer section 5.



Definition 1 (Decisional Supersingular Isogeny (DSSI) Problem). Given an additional curve $E_{\mathcal{S}}$ defined over $\mathbb{F}_{p^2}$, decide whether $E_{\mathcal{S}}$ is $\ell_{\mathcal{S}}^{e_{\mathcal{S}}}$-isogenous to E.

Definition 2 (Computational Supersingular Isogeny (CSSI) Problem). Given the curve $E_{\mathcal{S}}$ and the images $\phi_{\mathcal{S}}(P_{\mathcal{V}})$, $\phi_{\mathcal{S}}(Q_{\mathcal{V}})$, find a generator of $\langle P_{\mathcal{S}} + n_{\mathcal{S}} \cdot Q_{\mathcal{S}} \rangle$, where $\phi_{\mathcal{S}} : E \to E_{\mathcal{S}}$ is an isogeny with kernel $\langle P_{\mathcal{S}} + n_{\mathcal{S}} \cdot Q_{\mathcal{S}} \rangle$, and $n_{\mathcal{S}} \xleftarrow{\$} \mathbb{Z}/\ell_{\mathcal{S}}^{e_{\mathcal{S}}}\mathbb{Z}$.

Definition 3 (Supersingular Computational Diffie-Hellman (SSCDH) Problem). Let $\phi_{\mathcal{S}} : E \to E_{\mathcal{S}}$ and $\phi_{\mathcal{V}} : E \to E_{\mathcal{V}}$ be isogenies with kernel $\langle P_{\mathcal{S}} + n_{\mathcal{S}} \cdot Q_{\mathcal{S}} \rangle$ and $\langle P_{\mathcal{V}} + n_{\mathcal{V}} \cdot Q_{\mathcal{V}} \rangle$ respectively, where $n_{\mathcal{S}} \xleftarrow{\$} \mathbb{Z}/\ell_{\mathcal{S}}^{e_{\mathcal{S}}}\mathbb{Z}$ and $n_{\mathcal{V}} \xleftarrow{\$} \mathbb{Z}/\ell_{\mathcal{V}}^{e_{\mathcal{V}}}\mathbb{Z}$. Then, given the curves $E_{\mathcal{S}}, E_{\mathcal{V}}$ and the images $\phi_{\mathcal{S}}(P_{\mathcal{V}}), \phi_{\mathcal{S}}(Q_{\mathcal{V}}), \phi_{\mathcal{V}}(P_{\mathcal{S}}), \phi_{\mathcal{V}}(Q_{\mathcal{S}})$, find the j-invariant of

$$E/\langle P_{\mathcal{S}} + n_{\mathcal{S}} \cdot Q_{\mathcal{S}}, P_{\mathcal{V}} + n_{\mathcal{V}} \cdot Q_{\mathcal{V}} \rangle$$

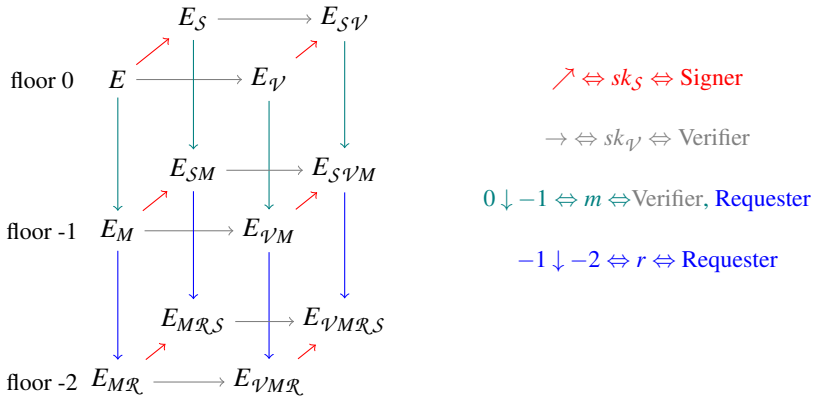
Definition 4 (Decisional Supersingular Product (DSSP) Problem). Given an isogeny $\phi : E \to E_3$ of degree $\ell_{\mathcal{S}}^{e_{\mathcal{S}}}$ and a tuple sampled with probability $1/2$ from one of the following distributions:
– (E_1, E_2, ϕ'): where the product $E_1 \times E_2$ is chosen randomly among $\ell_{\mathcal{V}}^{e_{\mathcal{V}}}$-isogenous couple to $E \times E_3$, and $\phi' : E_1 \to E_2$ is an isogeny of degree $\ell_{\mathcal{S}}^{e_{\mathcal{S}}}$
– (E_1, E_2, ϕ'): where E_1 is chosen randomly among the curves isogenous to E, and $\phi' : E_1 \to E_2$ is a random isogeny of degree $\ell_{\mathcal{S}}^{e_{\mathcal{S}}}$
then determine that the tuple is sampled from which of the above distributions.

Isogeny graphs allow to translate the problem of finding an isogeny between two given elliptic curves in the problem of finding paths between two nodes in a graph, which can be solved by a meet-in-the-middle approach in $O(\sqrt{n})$ time and memory, where n is the number of nodes in the graph. Biasse, Jao and Sankar [3] published in 2014 the first quantum algorithm to solve the general isogeny problem (GIP) between supersingular curves by random walks in the 3-isogeny graph. They reduced GIP to find an isogeny between two supersingular elliptic curves defined over $\mathbb{F}_p$ which can be solved in sub-exponential time. Specifically, they proved that there exists a quantum algorithm, to solve this problem, with complexity $\tilde{O}(p^{1/4})$ in the general case, and with $O(e^{\frac{\sqrt{3}}{2}\sqrt{\log(p)}\sqrt{\log\log(p)}})$ when both the curves are defined over $\mathbb{F}_p$. In the current state of the art, there is no specific algorithm that uses the additional information provided in CSSI, except an algorithm by Petit [26]. However, the hypotheses assumed in [26] are different from the hypotheses suggested by Jao and De Feo [18] to use isogenies of degree of the same size in order to maximize the security of SIDH.

3 A General Construction of DVS

In the DHKE protocol of [12] the zero knowledge proof (ZKP) of identity is provided by a commutative square diagram. An extended view of this approach can be seen in achieving confirmation and disavowal protocol, i.e. in verification, of the undeniable signature [19]. It is obtained through a 6-faced diagram i.e. a cube in which each of the face is a commutative diagram. The reason for it is straight forward. The scheme in [19] uses 3 primes over the 2 primes of [12]. In general extending this notion to arbitrary number of primes would render in realising a hypercube with each face having a commutative diagram. We investigate this fact to realize a signature scheme in a generic sense considering some functionalities of the signature. We start our investigation by considering the double cube, with a commutative square at each of the faces, as conceived in section 5 for the construction of our proposed SI-DVBS scheme.

The idea is as follows: each function involved contributes a path in a three-dimensional commutative diagram, in which, specific information are required to move in a specific direction.

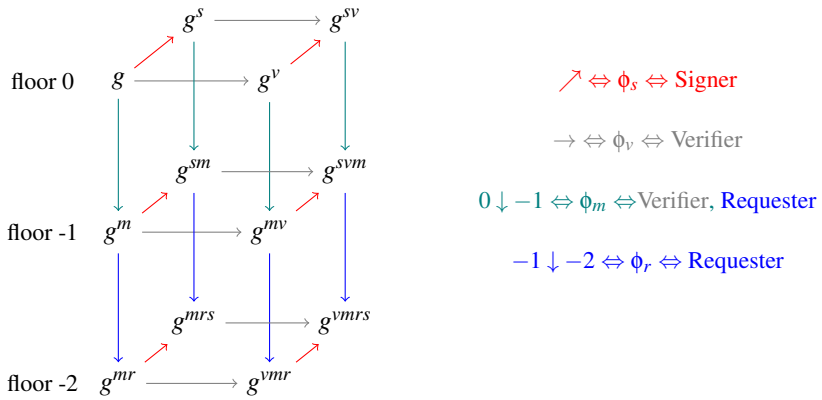


The lower cube is involved only in the Sign algorithm of our proposed scheme which essentially contains the *blinding* and *unblinding* phases. However, only the upper cube can be considered for signature, without considering the blindness property, as

$$\frac{E_{\mathcal{V}M}}{\langle \phi_{\mathcal{V}M}(\phi_{\mathcal{V}}(P_{\mathcal{S}})) + n_{\mathcal{S}} \cdot \phi_{\mathcal{V}M}(\phi_{\mathcal{V}}(Q_{\mathcal{S}})) \rangle}$$

hence, this way we generally obtain an isogeny-based *designated verifier* signature.

An interesting question is that, if this *double cube* model can be adopted each time to realize a Diffie-Hellman type primitive. For example, let us consider a cyclic group $G = \langle g \rangle$, in which the DLP is hard (suppose for now, not in the post-quantum context), and define the exponentiation automorphisms $\phi_x \colon G \to G$ such that $g \mapsto g^x$. We can build a similar commutative diagram in which the signer, verifier and requester can move following the similar rules, i.e.



Now, we can define Setup, KeyGen, Sign, Verify and TranSim as above by substituting the isogenies with the exponentiation maps. Let us consider the upper cube i.e the DVS part of the scheme[1]. Clearly this is not unforgeable, since if an adversary queries the signature $S = g^{svm}$ on a certain message $\mathtt{m}$, encoded as m, then he can recover g^{sv} as $S^{1/m}$ and can compute a valid signature for another message $\mathtt{m}'$ as $S^{m'/m}$. As a countermeasure, we can impose the signature to be hashed.

In particular, the idea of hashing is not an effective countermeasure when we want to achieve the blindness, since an adversary acting as requester must have access to S before the hashing, to unblind the signature. However, this idea of three-dimensional cube can be used to obtain a DVS based on DLP in general. Further, a similar approach can be adopted to achieve a DVS based on ECDLP.

Couveignes [9] introduced the notion of HHS, which is essentially a simple transitively action of finite group, some of whose operations are easy to compute and some are hard. He showed that from each HHS a Diffie-Hellman type protocol can be obtained naturally. In this view, we have that, from each HHS a DVS can be obtained naturally. An alternative isogeny-based cryptograpic primitive is commutative SIDH (CSIDH) [4], which at the current state of art, is an instance of HHS. More explicitly, in this case the objects are supersingular elliptic curves defined over $\mathbb{F}_p$ whose endomorphism ring over $\mathbb{F}_p$ is a given order O, in an imaginary quadratic field, and the arrows are the ideals of O. Thus, our construction provides also an DVS based on CSIDH.

We emphasise that our DVBS construction can be realised on SIDH setting but not on the CSIDH. The crucial issue is that to recover $E_{\mathcal{SV}}$ from a signature, additional information are required to compute the dual isogeny using the hash of the message.
An interesting problem is to understand if it is possible to modify our protocol to obtain a DVBS from HHS.

[1] Note that in the general setting requester and signer are the same person.

4 Supersingular Isogeny-Based Designated Verifier Blind Signature (SI-DVBS) Scheme

We present here the definition of a supersingular isogeny-based designated verifier blind signature (SI-DVBS) scheme and formalize a security model for it.

4.1 SI-DVBS Scheme

There are three users in the scheme: the *requester* $\mathcal{R}$ who requests signature, designated to a particular verifier, on a blinded message, from the signer; the *signer* $\mathcal{S}$ who signs the blinded messages for the requester and the *verifier* $\mathcal{V}$ who verifies the signature received from the requester. The SI-DVBS scheme consists of the following algorithms:

1. $params \leftarrow \mathsf{Setup}(\lambda)$: This is the *Setup* algorithm. On input security parameter λ, this algorithm generates the system's public parameters *params*. In all the algorithms from here onward, *params* will be considered as an implicit input.
2. $((pk_{\mathcal{S}}, sk_{\mathcal{S}}), (pk_{\mathcal{V}}, sk_{\mathcal{V}})) \leftarrow \mathsf{KeyGen}(params)$: This *key generation* algorithm, on input *params*, generates signer's and verifier's (public key, private key) pairs $(pk_{\mathcal{S}}, sk_{\mathcal{S}})$ and $(pk_{\mathcal{V}}, sk_{\mathcal{V}})$, respectively.
3. $\sigma \leftarrow \mathsf{Sign}(sk_{\mathcal{S}}, pk_{\mathcal{V}}, \mathtt{m})$: This is the *signature* algorithm. On input the signing key $sk_{\mathcal{S}}$ of signer, public key $pk_{\mathcal{V}}$ of verifier and the message $\mathtt{m}$, this probabilistic (or deterministic) algorithm finally generates a SI-DVBS, σ. The main algorithm consists of the following three sub-algorithms:
   (a) $\mathtt{m}' \leftarrow \mathsf{Blinding}(\mathtt{m}, r, pk_{\mathcal{V}})$: This is a probabilistic *blinding* algorithm, run by the requester, which outputs the *blinded message* $\mathtt{m}'$ depending on the input message $\mathtt{m}$, a random choice r and the public keys $pk_{\mathcal{V}}$ of the verifier.
   (b) $\sigma' \leftarrow \mathsf{Sign}(\mathtt{m}', sk_{\mathcal{S}})$: This is a signing algorithm run by the signer, which takes input the blinded message $\mathtt{m}'$ and signer's secret key $sk_{\mathcal{S}}$. This algorithm outputs signature σ' on the blinded message $\mathtt{m}'$.
   (c) $\sigma \leftarrow \mathsf{Unblinding}(\sigma', r)$: This is a deterministic *unblinding* algorithm , run by the requester, which outputs the unblinded signature σ on message $\mathtt{m}$, taking input the blinded signature σ' and the random choice r.
4. $b \leftarrow \mathsf{Verify}(sk_{\mathcal{V}}, pk_{\mathcal{S}}, \sigma, \mathtt{m})$: This is a deterministic *verification* algorithm run by the designated verifier. On input secret key $sk_{\mathcal{V}}$ of the verifier, public key $pk_{\mathcal{S}}$ of signer, signature σ and message $\mathtt{m}$, this algorithm outputs a bit b which is 1 if the signature is valid and 0 if invalid.
5. $\hat{\sigma} \leftarrow \mathsf{TranSim}(sk_{\mathcal{V}}, pk_{\mathcal{S}}, \mathtt{m})$: This is a deterministic *transcript simulation* algorithm run by the designated verifier. On input secret key $sk_{\mathcal{V}}$ of the verifier, public key $pk_{\mathcal{S}}$ of the signer and message $\mathtt{m}$, this algorithm outputs identically distributed transcript that is indistinguishable from the original signature.

Remark 1. In practice we can be interested to give the signer the possibility to have control on the verifier. More specifically, if we add to the input of 3.(b) explicitly the identity of the verifier, the signer can decide to sign, or refuse to sign a message for such designated verifier.

4.2 Security Properties for SI-DVBS

A secure SI-DVBS scheme must satisfy the following properties.

1. *Correctness*: If the signature σ on a message $\mathtt{m}$ is correctly computed (i.e. signed correctly on the blinded message $\mathtt{m}'$ by the signer $\mathcal{S}$ and unblinded correctly by the requester $\mathcal{R}$), then the designated verifier $\mathcal{V}$ must be able to verify the correctness of the (message, signature) pair $(\mathtt{m},\sigma)$. That is,

$$\Pr[1 \leftarrow \mathsf{Verify}(sk_{\mathcal{V}}, pk_{\mathcal{S}}, \mathsf{Sign}(sk_{\mathcal{S}}, pk_{\mathcal{S}}, pk_{\mathcal{V}}, \mathtt{m}), \mathtt{m})] = 1.$$

where $\mathsf{Sign}(sk_{\mathcal{S}}, pk_{\mathcal{S}}, pk_{\mathcal{V}}, \mathtt{m}) = \sigma$.

2. *Unforgeability*: It is computationally infeasible to construct a valid SI-DVBS without the knowledge of private key of either the signer or the designated verifier.

3. *Blindness*: The signer should not be able to correspond the (message, signature) pairs to their blinded copies.

Definition 5 (Blindness). An SI-DVBS scheme is said to achieve blindness if for any PPT adversary $\mathcal{A}$ which runs in time t, the advantage

$$\mathrm{Adv}^{\text{BLIND-CMA2}}_{\text{SI-DVBS},\mathcal{A}}(\lambda) := \varepsilon_{\mathcal{A}}(\lambda) := |\Pr[b' = b] - \frac{1}{2}|$$

is negligible in λ in the below game. We consider the security game motivated by [30,33].

1. *Setup*: On input a security parameter λ, the challenger $\mathcal{C}$ runs $\mathsf{KeyGen}(\lambda)$ to generate the public parameter *params* and the system key pair (pk, sk) and gives the adversary $\mathcal{A}$ the public key pk.
2. *Challenge*: $\mathcal{A}$ outputs two messages m_0 and m_1 and sends them to $\mathcal{C}$. Receiving these messages, $\mathcal{C}$ picks a random bit $b \xleftarrow{\$} \{0,1\}$ and reorder the messages as $(m_b, m_{(1-b)})$, blind them as $m'_b = Blind(m_b, r_1)$ and $m'_{(1-b)} = Blind(m_{(1-b)}, r_2)$. r_1, r_2 are chosen at random. $\mathcal{C}$ then gives m'_b and $m'_{(1-b)}$ to $\mathcal{A}$ as the challenge blinded messages.
3. *Queries*: $\mathcal{A}$ then obtain the following responses by accessing the corresponding oracles:
   - $\mathcal{A}$ access the Sign oracle for inputs m'_b and $m'_{(1-b)}$, and receives σ'_b, $\sigma'_{(1-b)}$.
   - $\mathcal{A}$ sends σ'_b and $\sigma'_{(1-b)}$ to the challenger $\mathcal{C}$ and receives σ_b and $\sigma_{(1-b)}$ as the corresponding unblinded signatures.
4. *Guess*: Finally $\mathcal{A}$ outputs its guess b' for b.

4.*Unverifiability*: It is computationally infeasible to verify the validity of a SI-DVBS without the knowledge of the private key of either the signer or the designated verifier.

5. *Non-transferability*: This property establish the fact that the designated verifier cannot transfer the conviction of the verification to any third party. This is due to the fact

that the verifier can output a signature, during the simulation in the TranSim phase, indistinguishable from the DVBS obtained in the Sign protocol. More formally, given a DVBS (i.e. σ) on message $\mathtt{m}$, it is infeasible for any PPT adversary $\mathcal{A}$ to decide whether σ was produced by the signer or by the designated verifier, even if $\mathcal{A}$ is also given the private keys of the signer and the designated verifier.

Definition 6 (Non-transferability). An SI-DVBS scheme is said to achieve non- transferability if the signature generated by the signer is computationally indistinguishable from that generated by the designated verifier, that is,

$$\sigma \leftarrow \mathsf{Sign}(sk_{\mathcal{S}}, pk_{\mathcal{V}}, \mathtt{m}) \approx \widehat{\sigma} \leftarrow \mathsf{TranSim}(sk_{\mathcal{V}}, pk_{\mathcal{S}}, \mathtt{m}).$$

5 Proposed Scheme

In this section, we present our proposed SI-DVBS. As described in section 4, the proposed scheme consists of the algorithms: Setup, KeyGen, Sign,Verify and TranSim.

Setup**:** Given a security parameter λ, the algorithm generates system's public parameters

$$params = (p, E, \{P_{\mathcal{R}}, Q_{\mathcal{R}}\}, \{P_{\mathcal{S}}, Q_{\mathcal{S}}\}, \{P_{\mathcal{V}}, Q_{\mathcal{V}}\}, \{P_M, Q_M\}, H)$$

where $p = p(\lambda)$ is a prime of the form $\ell_{\mathcal{R}}^{e_{\mathcal{R}}} \ell_{\mathcal{S}}^{e_{\mathcal{S}}} \ell_{\mathcal{V}}^{e_{\mathcal{V}}} \ell_M^{e_M} \cdot f \pm 1$, ℓ_i are small primes and f is a co-factor such that p is prime, E is a supersingular elliptic curve over $\mathbb{F}_{p^2}$ such that $\#E(\mathbb{F}_{p^2})$ is divisible by $(\ell_{\mathcal{R}}^{e_{\mathcal{R}}} \ell_{\mathcal{S}}^{e_{\mathcal{S}}} \ell_{\mathcal{V}}^{e_{\mathcal{V}}} \ell_M^{e_M})^2$, $\{P_{\mathcal{R}}, Q_{\mathcal{R}}\}, \{P_{\mathcal{S}}, Q_{\mathcal{S}}\}$, $\{P_{\mathcal{V}}, Q_{\mathcal{V}}\}, \{P_M, Q_M\}$ are bases of $E[\ell_{\mathcal{R}}^{e_{\mathcal{R}}}], E[\ell_{\mathcal{S}}^{e_{\mathcal{S}}}], E[\ell_{\mathcal{V}}^{e_{\mathcal{V}}}], E[\ell_M^{e_M}]$ respectively, and H is cryptographic hash function defined as $H : \{0,1\}^* \rightarrow \frac{\mathbb{Z}}{\ell_M^{e_M}\mathbb{Z}}$.

Remark 2. Since the security of our protocol relies on the hardness of computing isogenies, consistently with the literature, we consider the scheme achieving the security level λ if p satisfies certain conditions, mentioned further in section 6.

KeyGen**:** The signer and the verifier generate their respective public key and private key as follows:

- The signer randomly selects $n_{\mathcal{S}} \in \mathbb{Z}/\ell_{\mathcal{S}}^{e_{\mathcal{S}}}\mathbb{Z}$, computes the cyclic subgroup $\mathcal{K}_{\mathcal{S}} = \langle P_{\mathcal{S}} + n_{\mathcal{S}} \cdot Q_{\mathcal{S}} \rangle \subset E$ and the isogeny $\phi_{\mathcal{S}} : E \longrightarrow E_{\mathcal{S}}$ were $E_{\mathcal{S}}$ is a representative of the class of curves $E/\mathcal{K}_{\mathcal{S}}$. The public and private key of the signer are as follows:
  $pk_{\mathcal{S}} \leftarrow E_{\mathcal{S}}, \phi_{\mathcal{S}}(P_{\mathcal{V}}), \phi_{\mathcal{S}}(Q_{\mathcal{V}}), \phi_{\mathcal{S}}(P_M), \phi_{\mathcal{S}}(Q_M)$
  $sk_{\mathcal{S}} \leftarrow n_{\mathcal{S}}$ (or equivalently $\mathcal{K}_{\mathcal{S}}$ or $\phi_{\mathcal{S}}$)
- The verifier randomly selects $n_{\mathcal{V}} \in \mathbb{Z}/\ell_V^{e_{\mathcal{V}}}\mathbb{Z}$, computes the cyclic subgroup $\mathcal{K}_{\mathcal{V}} = \langle P_{\mathcal{V}} + n_{\mathcal{V}} \cdot Q_{\mathcal{V}} \rangle \subset E$ and the isogeny $\phi_{\mathcal{V}} : E \longrightarrow E_{\mathcal{V}}$ were $E_{\mathcal{V}}$ is a representative of the class of curves $E/\mathcal{K}_{\mathcal{V}}$. The public and private key of the verifier are as follows:
  $pk_{\mathcal{V}} \leftarrow E_{\mathcal{V}}, \phi_{\mathcal{V}}(P_M), \phi_{\mathcal{V}}(Q_M), \phi_{\mathcal{V}}(P_{\mathcal{S}}), \phi_{\mathcal{V}}(Q_{\mathcal{S}}), \phi_{\mathcal{V}}(P_{\mathcal{R}}), \phi_{\mathcal{V}}(Q_{\mathcal{R}})$
  $sk_V \leftarrow n_{\mathcal{V}}$ (or equivalently $\mathcal{K}_{\mathcal{V}}$ or $\phi_{\mathcal{V}}$)

Sign: To get a DVBS on message $\mathtt{m}$, the requester $\mathcal{R}$ first blinds the message and sends it to the signer $\mathcal{S}$, who signs the blinded message and sends back to $\mathcal{R}$. Finally, $\mathcal{R}$ unblinds the signature received from the signer, to output signature on $\mathtt{m}$. The following algorithms describe this process:

(a) Blinding:
Hashing : Let $\mathtt{m}$ be the message to be signed. The requester computes the hash $h = H(\mathtt{m})$ and the isogeny $\phi_{\mathcal{V}M}$ whose co-domain is the curve

$$E_{\mathcal{V}M} = \frac{E_{\mathcal{V}}}{\langle \phi_{\mathcal{V}}(P_M) + h \cdot \phi_{\mathcal{V}}(Q_M) \rangle}$$

Additionally the following images are computed

$$\phi_{\mathcal{V}M}(\phi_{\mathcal{V}}(P_{\mathcal{R}})), \phi_{\mathcal{V}M}(\phi_{\mathcal{V}}(Q_{\mathcal{R}})), \phi_{\mathcal{V}M}(\phi_{\mathcal{V}}(P_{\mathcal{S}})), \phi_{\mathcal{V}M}(\phi_{\mathcal{V}}(Q_{\mathcal{S}}))$$

$$\begin{array}{ccc} E & \overset{\phi_{\mathcal{V}}}{\dashrightarrow} & E_{\mathcal{V}} \\ & & \downarrow{\scriptstyle \phi_{\mathcal{V}M}} \\ & & E_{\mathcal{V}M} \end{array}$$

Blinding : The requester selects $r \in \mathbb{Z}/\ell_{\mathcal{R}}^{e_{\mathcal{R}}}\mathbb{Z}$ randomly and computes the isogeny $\phi_{\mathcal{V}M\mathcal{R}}$ whose co-domain is

$$E_{\mathcal{V}MR} = \frac{E_{\mathcal{V}M}}{\langle \phi_{\mathcal{V}M}(\phi_{\mathcal{V}}(P_{\mathcal{R}})) + r \cdot \phi_{\mathcal{V}M}(\phi_{\mathcal{V}}(Q_{\mathcal{R}})) \rangle}$$

$$\begin{array}{ccc} E & \overset{\phi_{\mathcal{V}}}{\dashrightarrow} & E_{\mathcal{V}} \\ & & \downarrow{\scriptstyle \phi_{\mathcal{V}M}} \\ & & E_{\mathcal{V}M} \\ & & \downarrow{\scriptstyle \phi_{\mathcal{V}M\mathcal{R}}} \\ & & E_{\mathcal{V}M\mathcal{R}} \end{array}$$

Remark 3. Inspired by [33], now we need to compute the dual of $\phi_{\mathcal{V}M\mathcal{R}}$ to make the unblinding possible. More precisely it is sufficient for our purpose that the requester finds the inverse of this map in the isogeny graph. In what follows we are writing $\hat{\phi}_{\mathcal{V}M\mathcal{R}}$ for such a map and identifying the co-domain $E_{\mathcal{V}M}$ little improperly, since such $E_{\mathcal{V}M}$ is defined up to isomorphism. We refer to [33] for details (see Section 4 and Remark 4.1) and recall the main operations in order to establish a coherent notation in our setting.

The requester has to find a point $K_{\mathcal{V}} \in E_{\mathcal{V}M}[\ell_{\mathcal{R}}^{e_{\mathcal{R}}}]$ of order exactly $\ell_{\mathcal{R}}^{e_{\mathcal{R}}}$ such that $K_{\mathcal{V}} \notin \ker \phi_{\mathcal{V}M\mathcal{R}}$. Then he sets $\ker \hat{\phi}_{\mathcal{V}M\mathcal{R}} = \langle \phi_{\mathcal{V}M\mathcal{R}}(K_{\mathcal{V}}) \rangle$. Now he chooses a random basis $\left\{P'_{\mathcal{R}}, Q'_{\mathcal{R}}\right\}$ of $E_{\mathcal{V}M\mathcal{R}}[\ell_{\mathcal{R}}^{e_{\mathcal{R}}}]$ and computes $m, n \in \mathbb{Z}/\ell_{\mathcal{R}}^{e_{\mathcal{R}}}\mathbb{Z}$ such that

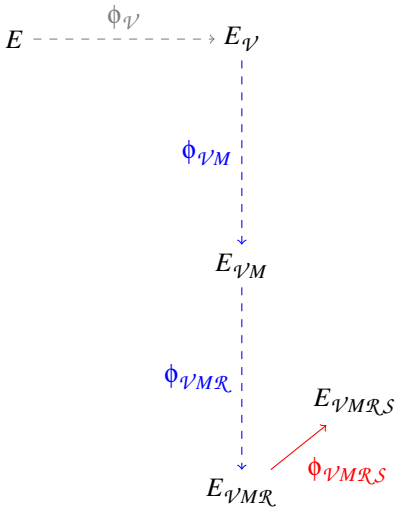
$$\phi_{\mathcal{V}M\mathcal{R}}(K_{\mathcal{V}}) = m \cdot P'_{\mathcal{R}} + n \cdot Q'_{\mathcal{R}}$$

The masking curve $E_{\mathcal{V}M\mathcal{R}}$, the tuple $\left\{P'_{\mathcal{R}}, Q'_{\mathcal{R}}\right\}$ and the following images are sent to the signer

$$\phi_{\mathcal{V}M\mathcal{R}}(\phi_{\mathcal{V}M}(\phi_{\mathcal{V}}(P_{\mathcal{S}}))), \phi_{\mathcal{V}M\mathcal{R}}(\phi_{\mathcal{V}M}(\phi_{\mathcal{V}}(Q_{\mathcal{S}}))).$$

(b) Sign : The signer computes the curve

$$E_{\mathcal{V}M\mathcal{R}\mathcal{S}} = \frac{E_{\mathcal{V}M\mathcal{R}}}{\langle \phi_{\mathcal{V}M\mathcal{R}}(\phi_{\mathcal{V}M}(\phi_{\mathcal{V}}(P_{\mathcal{S}}))) + n_{\mathcal{S}} \cdot \phi_{\mathcal{V}M\mathcal{R}}(\phi_{\mathcal{V}M}(\phi_{\mathcal{V}}(Q_{\mathcal{S}})))\rangle}$$

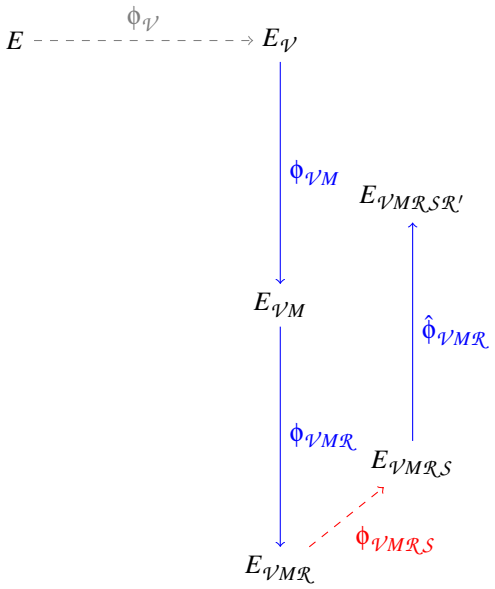


and provides $E_{\mathcal{V}M\mathcal{R}\mathcal{S}}$, $\phi_{\mathcal{V}M\mathcal{R}\mathcal{S}}(P'_{\mathcal{R}})$ and $\phi_{\mathcal{V}M\mathcal{R}\mathcal{S}}(Q'_{\mathcal{R}})$ to the requester as her signature on the blinded message $E_{\mathcal{V}M\mathcal{R}}$.

(c) Unblinding: Receiving the signature on the blinded message, the requester generates the signature on the original message $\mathtt{m}$, by computing

$$E_{\mathcal{V}M\mathcal{R}\mathcal{S}\mathcal{R}'} = \frac{E_{\mathcal{V}M\mathcal{R}\mathcal{S}}}{\langle m \cdot \phi_{\mathcal{V}M\mathcal{R}\mathcal{S}}(P'_{\mathcal{R}}) + n \cdot \phi_{\mathcal{V}M\mathcal{R}\mathcal{S}}(Q'_{\mathcal{R}})\rangle}$$

and sends the signature $\sigma = (\mathtt{m}, j(E_{\mathcal{V}M\mathcal{R}\mathcal{S}\mathcal{R}'}))$ to the designated verifier $\mathcal{V}$.



Verify : To verify the received signature σ on the message $\mathtt{m}$, the designated verifier first computes $h = H(\mathtt{m})$ then proceeds by computing the curves

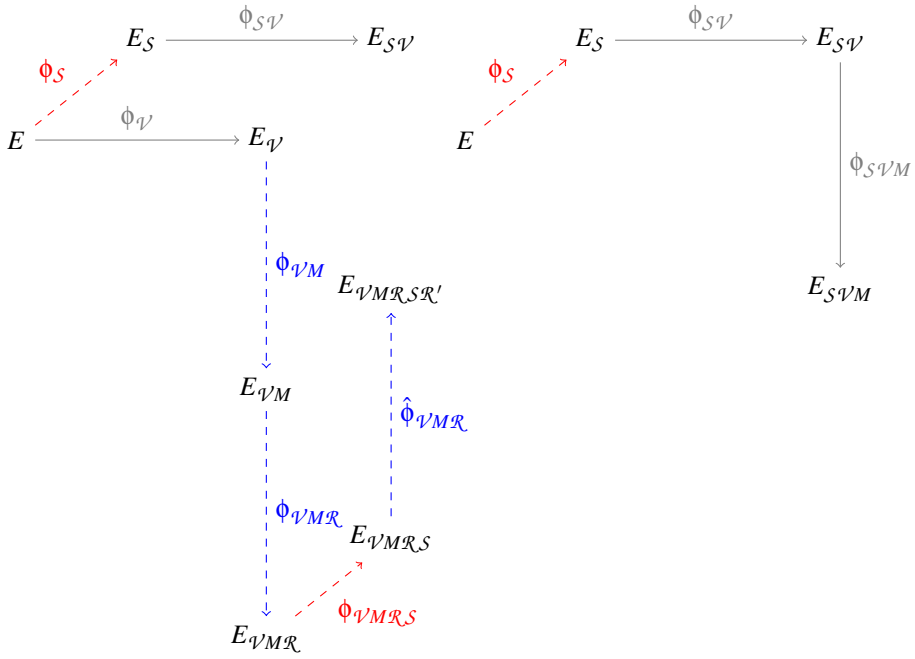
$$E_{\mathcal{S}\mathcal{V}} = \frac{E_{\mathcal{S}}}{\langle \phi_{\mathcal{S}}(P_{\mathcal{V}}) + n_{\mathcal{V}} \cdot \phi_{\mathcal{S}}(Q_{\mathcal{V}}) \rangle}$$

and

$$E_{\mathcal{S}\mathcal{V}M} = \frac{E_{\mathcal{S}\mathcal{V}}}{\langle \phi_{\mathcal{S}\mathcal{V}}(\phi_{\mathcal{S}}(P_M)) + h \cdot \phi_{\mathcal{S}\mathcal{V}}(\phi_{\mathcal{S}}(Q_M)) \rangle}.$$

Finally, the verifier accepts σ as a valid signature on message $\mathtt{m}$ if and only if

$$j(E_{\mathcal{V}M\mathcal{R}\mathcal{S}\mathcal{R}'}) = j(E_{\mathcal{S}\mathcal{V}M})$$



TranSim : To output identically distributed transcripts indistinguishable from the received signature $\sigma = E_{\mathcal{VMRSR'}}$ on a message $\mathtt{m}$, the designated verifier proceeds exactly in the same manner as the Verify algorithm, and computes a simulated signature $\hat{\sigma}$ i.e. an elliptic curve isomorphic to $E_{\mathcal{VMRSR'}}$

6 Analysis of the Proposed Scheme

6.1 Correctness of the Proposed Scheme

The proposed SI-DVBS scheme is correct, as the curve $E_{\mathcal{VMRSR'}}$ is isomorphic to the curve $E_{\mathcal{SVM}}$, thus their corresponding j-invariants are same

$$j(E_{\mathcal{VMRSR'}}) = j(E_{\mathcal{SVM}}).$$

6.2 Unforgeability

Following the security requirements formalized in section 4, we recall that the property of unforgeability achieves the fact that no one, except the signer and the designated verifier, can output an SI-DVBS which follows the verification correctly. In connection to the most relevant works [19,33], we emphasise that in contrast to the interactive zero-knowledge proof adopted in [33] following the techniques of [19], unforgeability of our scheme corresponds to the notion in achieving *completeness, zero-knowledge (NIZK)* and *simulation-sound online-extractability* as described in [38] towards realizing NIZK proof in quantum random oracle, as the presented signature is non-interactive.

6.3 Blindness

We prove here that the proposed DVBS scheme achieves blindness following the model formalized in section 4.2.

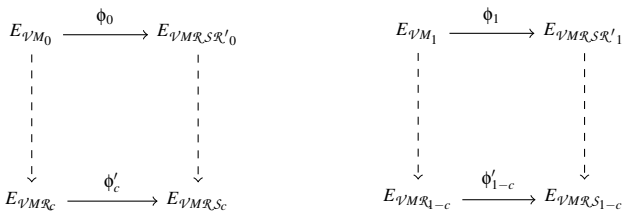
1. *Setup*: For security parameter λ, the challenger $\mathcal{C}$ provides *params*

$$(p, E, \{P_{\mathcal{R}}, Q_{\mathcal{R}}\}, \{P_{\mathcal{S}}, Q_{\mathcal{S}}\}, \{P_{\mathcal{V}}, Q_{\mathcal{V}}\}, \{P_M, Q_M\}, H)$$

and public keys
$pk_{\mathcal{S}}$: $E_{\mathcal{S}}, \phi_{\mathcal{S}}(P_{\mathcal{V}}), \phi_{\mathcal{S}}(Q_{\mathcal{V}}), \phi_{\mathcal{S}}(P_M), \phi_{\mathcal{S}}(Q_M)$
$pk_{\mathcal{V}}$: $E_{\mathcal{V}}, \phi_{\mathcal{V}}(P_M), \phi_{\mathcal{V}}(Q_M), \phi_{\mathcal{V}}(P_{\mathcal{S}}), \phi_{\mathcal{V}}(Q_{\mathcal{S}}), \phi_{\mathcal{V}}(P_{\mathcal{R}}), \phi_{\mathcal{V}}(Q_{\mathcal{R}})$
to the adversary $\mathcal{A}$.

2. *Challenge*: $\mathcal{A}$ outputs two messages $\mathtt{m}_0$ and $\mathtt{m}_1$ and sends them to $\mathcal{C}$. Receiving these messages, $\mathcal{C}$ picks a random bit $b \xleftarrow{\$} \{0,1\}$ and reorder the messages as $(\mathtt{m}_b, \mathtt{m}_{(1-b)})$, computes $E_{\mathcal{V}M\mathcal{R}_b} = \mathsf{Blinding}(\mathtt{m_b}, \mathtt{r_1})$ and $E_{\mathcal{V}M\mathcal{R}_{(1-b)}} = \mathsf{Blinding}(\mathtt{m_{(1-b)}}, \mathtt{r_2})$ and sends these curves to $\mathcal{A}$ as the challenge blinded messages.

3. *Queries*: $\mathcal{A}$ get access to two parallel interactive (Sign) protocols and finally receives two curves $E_{\mathcal{V}M\mathcal{R}\mathcal{S}\mathcal{R}'_0}$ and $E_{\mathcal{V}M\mathcal{R}\mathcal{S}\mathcal{R}'_1}$ from the challenger as unblinded signatures. Precisely, during these interactive protocols the adversary $\mathcal{A}$ gets knowledge of the curves:
– $E_{\mathcal{V}M_0}, E_{\mathcal{V}M\mathcal{R}\mathcal{S}\mathcal{R}'_0}$ and isogeny ϕ_0 between them.
– $E_{\mathcal{V}M_1}, E_{\mathcal{V}M\mathcal{R}\mathcal{S}\mathcal{R}'_1}$ and isogeny ϕ_1 between them.
– $E_{\mathcal{V}M\mathcal{R}_c}, E_{\mathcal{V}M\mathcal{R}\mathcal{S}_c}$ and isogeny ϕ'_c between them.
– $E_{\mathcal{V}M\mathcal{R}_{1-c}}, E_{\mathcal{V}M\mathcal{R}\mathcal{S}_{1-c}}$ and isogeny ϕ'_{1-c} between them.
such that there exists $c \in \{0,1\}$ (depending on b) providing the following commutative diagrams:



5. *Guess*: Finally $\mathcal{A}$ outputs the value of bit b.

Solution of DSSP Problem: By the knowledge of above curves and corresponding isogeies between them, it is straight forward that if the adversary $\mathcal{A}$ outputs correct value of bit b, then the challenger $\mathcal{C}$ can output solution of the DSSP problem using all the responses obtained by the adversary, as correctly deciding the value of b is equivalent to deciding whether $E_{\mathcal{V}M\mathcal{R}_1} \times E_{\mathcal{V}M\mathcal{R}\mathcal{S}_1}$ is $\ell_{\mathcal{R}}^{e_{\mathcal{R}}}$-isogenous to $E_{\mathcal{V}M_1} \times E_{\mathcal{V}M\mathcal{R}\mathcal{S}\mathcal{R}'_1}$ or not, i.e. to solve an instance of DSSP problem.

6.4 Unverifiability

To verify the signature one has to compute the elliptic curve $E_{\mathcal{SVM}}$ from the knowledge of *params* and provided public keys. It is evident from the scheme described in section 5, that computation of curve $E_{\mathcal{SV}}$, isogenous to $E_{\mathcal{S}}$ requires the knowledge of private key $n_{\mathcal{V}}$ of the designated verifier, which leads further the computation of curve $E_{\mathcal{SVM}}$ isogenous to $E_{\mathcal{SV}}$. Thus, it is evident that no user without the private key of the designated verifier can actually verify the validity of the signature. Moreover, since a transcript, indistinguishable to the proposed signature, can be simulated by the verifier, the same fact applies for the signer (when she acts as a verifier for the simulated transcript), hence, following the definition of *unverifiability* from section 4, it can be established that it is computationally infeasible to verify the validity of the proposed SI-DVBS without the knowledge of the private key of either the signer or the designated verifier.

6.5 Non-transferability

As described in section 4, the property of non-transferability implies that the signatures simulated by the designated verifier are indistinguishable from those that he receives from the signer. TranSim phase of Section 5 already shows that this property is achieved in the presented scheme.

6.6 Parameter Selection

The security of the proposed signature scheme relies on the problems related to computing an isogeny between two given supersingular elliptic curves. As in SIDH, the degree of the isogenies involved in our scheme are public. In order to compute an isogeny of degree ℓ^e between two given curves, the best (classic) solution is to explore the ℓ-isogeny graph using a meet-in-the-middle strategy. In our case, to achieve the maximal security against this attack, we have to maximize the minimum of $(O(\ell_{\mathcal{V}}^{e_{\mathcal{V}}}), O(\ell_{\mathcal{S}}^{e_{\mathcal{S}}}))$. Moreover, to achieve the maximal blindness, we have to maximize $O(\ell_{\mathcal{R}}^{e_{\mathcal{R}}})$. Unlike the SIDH, we reveal more information in the public key of the signer and the verifier. In particular, we reveal the image of some N-torsion subgrups (for N greater than the degree of the secret isognenies). Note that it is not possible to set the parameter as in SIDH, since here the public parameters are unbalanced. We suggest to use $\ell_{\mathcal{V}}^{e_{\mathcal{V}}} \approx \ell_{\mathcal{S}}^{e_{\mathcal{S}}} \approx \ell_{M}^{e_M} \approx p^{2/7}$ and $\ell_{\mathcal{R}}^{e_{\mathcal{R}}} \approx p^{1/7}$ and to set the initial curve E such that any non-trivial endomorphism is unknown. Currently, to generate such a curve the best way is to consider a random walk in the isogeny graph, however this operation must be performed by a trusted authority since it reveals information on the endomorphism ring of E. This choice of parameter is valid also in the quantum setting.

7 Conclusion

Designated verifier signature belongs to a special family of digital signature where a document can be signed particularly for a designated recipient in such a way that only

the authorised verifier can validate the signature but cannot transfer the conviction of verification to any third party. Blind signature is a candidate digital signature to provide user's anonymity. Now there may be situations where both these properties– anonymity and signer's control in the verification– may require together, for example in online anonymous auctions, electronic tendering and voting. In particular, Srinath and Chandrasekaran [33] have proposed undeniable blind signature scheme (UBSS) from supersingular isogeny for such a purpose. However, it has been observed that the undeniable signature suffers by some well known weaknesses and limitations which can be addressed by a designated verifier signature (DVS). In this paper, we have proposed a designated verifier blind signature from supersingular isogenies, which achieves similar properties as UBBS. Moreover, in contrast to the only existing SI-UBSS we do not require interactive communications between the signer and the verifier i.e. we eliminate the communication overhead. Additionally, we have also formalized a generic construction of a DVS from hard homogenous spaces and have discussed the possibility of realization of a DVS under different security assumptions.

References

1. Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.
2. Jean-François Biasse, David Jao, and Anirudh Sankar. A quantum algorithm for computing isogenies between supersingular elliptic curves. In *International Conference in Cryptology in India*, pages 428–442. Springer, 2014.
3. Jean-François Biasse, David Jao, and Anirudh Sankar. A quantum algorithm for computing isogenies between supersingular elliptic curves. In *International Conference in Cryptology in India*, pages 428–442. Springer, 2014.
4. Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. Csidh: An efficient post-quantum commutative group action. In Thomas Peyrin and Steven Galbraith, editors, *Advances in Cryptology ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Proceedings*, pages 395–427, 2018.
5. Denis Charles, Eyal Goren, and Kristin Lauter. Cryptographic hash functions from expander graphs. Cryptology ePrint Archive, Report 2006/021, 2006. `https://eprint.iacr.org/2006/021`.
6. David Chaum. Blind signatures for untraceable payments. In *Advances in cryptology*, pages 199–203. Springer, 1983.
7. David Chaum and Hans Van Antwerpen. Undeniable signatures. In *Conference on the Theory and Application of Cryptology*, pages 212–216. Springer, 1989.
8. Andrew Childs, David Jao, and Vladimir Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *Journal of Mathematical Cryptology*, 8(1):1–29, 2014.
9. Jean-Marc Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291, 2006. `https://eprint.iacr.org/2006/291`.
10. Yvo Desmedt, Claude Goutier, and Samy Bengio. Special uses and abuses of the fiat-shamir passport protocol. In *Conference on the Theory and Application of Cryptographic Techniques*, pages 21–39. Springer, 1987.

11. Yvo Desmedt and Moti Yung. Weaknesses of undeniable signature schemes. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 205–220. Springer, 1991.
12. Luca De Feo, David Jao, and Jrme Plt. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Cryptology ePrint Archive, Report 2011/506, 2011. https://eprint.iacr.org/2011/506.
13. Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Conference on the Theory and Application of Cryptographic Techniques*, pages 186–194. Springer, 1986.
14. Steven D Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 3–33. Springer, 2017.
15. Jeffrey Hoffstein, Jill Pipher, and Joseph H Silverman. Ntru: A ring-based public key cryptosystem. In *International Algorithmic Number Theory Symposium*, pages 267–288. Springer, 1998.
16. Markus Jakobsson. Blackmailing using undeniable signatures. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 425–427. Springer, 1994.
17. Markus Jakobsson, Kazue Sako, and Russell Impagliazzo. Designated verifier proofs and their applications. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 143–154. Springer, 1996.
18. David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *PQCrypto*, 7071:19–34, 2011.
19. David Jao and Vladimir Soukharev. Isogeny-based quantum-resistant undeniable signatures. In *International Workshop on Post-Quantum Cryptography*, pages 160–179. Springer, 2014.
20. Ari Juels, Michael Luby, and Rafail Ostrovsky. Security of blind digital signatures. In Burton S. Kaliski, editor, *Advances in Cryptology — CRYPTO '97*, pages 150–164, Berlin, Heidelberg, 1997. Springer Berlin Heidelberg.
21. Wenbo Mao. *Modern cryptography: theory and practice*. Pearson Education India, 2003.
22. Robert J McEliece. A public-key cryptosystem based on algebraic. *Coding Thv*, 4244:114–116, 1978.
23. R.C. Merkle. *Secrecy, Authentication, and Public Key Systems*. Computer Science Series. UMI Research Press, 1982.
24. Simon-Philipp Merz, Romy Minko, and Christophe Petit. Another look at some isogeny hardness assumptions. Cryptology ePrint Archive, Report 2019/950, 2019. https://eprint.iacr.org/2019/950.
25. Jacques Patarin. Hidden fields equations (hfe) and isomorphisms of polynomials (ip): Two new families of asymmetric algorithms. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 33–48. Springer, 1996.
26. Christophe Petit. Faster algorithms for isogeny problems using torsion point images. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 330–353. Springer, 2017.
27. David Pointcheval and Jacques Stern. Security arguments for digital signatures and blind signatures. *Journal of cryptology*, 13(3):361–396, 2000.
28. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):34, 2009.
29. Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. *IACR Cryptology ePrint Archive*, 2006:145, 2006.
30. Dominique Schröder and Dominique Unruh. Security of blind signatures revisited. *Journal of Cryptology*, 30(2):470–494, 2017.

31. Peter W Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, pages 124–134. Ieee, 1994.
32. Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.
33. M Seshadri Srinath and V Chandrasekaran. Isogeny-based quantum-resistant undeniable blind signature scheme. *IACR Cryptology ePrint Archive*, 2016:148, 2016.
34. Anton Stolbunov. Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves. *Adv. in Math. of Comm.*, 4(2):215–235, 2010.
35. Anton Stolbunov. Cryptographic schemes based on isogenies. 2012.
36. Xi Sun, Haibo Tian, and Yumin Wang. Toward quantum-resistant strong designated verifier signature from isogenies. In *Intelligent Networking and Collaborative Systems (INCoS), 2012 4th International Conference on*, pages 292–296. IEEE, 2012.
37. John Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones mathematicae*, 2(2):134–144, 1966.
38. Dominique Unruh. Non-interactive zero-knowledge proofs in the quantum random oracle model. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 755–784. Springer, 2015.
39. Jacques Vélu. Isogénies entre courbes elliptiques. *CR Acad. Sc. Paris.*, 273:238–241, 1971.
40. Lawrence C Washington. *Elliptic curves: number theory and cryptography*. Chapman and Hall/CRC, 2003.
41. Youngho Yoo, Reza Azarderakhsh, Amir Jalali, David Jao, and Vladimir Soukharev. A post-quantum digital signature scheme based on supersingular isogenies. In *International Conference on Financial Cryptography and Data Security*, pages 163–181. Springer, 2017.
42. Ning Zhang and Qiaoyan Wen. Provably secure blind id-based strong designated verifier signature scheme. In *CHINACOM'07*, pages 323–327. IEEE, 2007.