

ISOGENY-BASED QUANTUM-RESISTANT UNDENIABLE BLIND SIGNATURE SCHEME

SRINATH M. S. AND V. CHANDRASEKARAN

ABSTRACT. In this paper, we propose an Undeniable Blind Signature scheme (UBSS) based on isogenies between supersingular elliptic curves. The proposed UBSS is an extension of the Jao-Soukharev undeniable signature scheme [19]. We formalize the notion of a UBSS by giving the formal definition. We then study its properties along with the pros and cons. Based on this, we provide a couple of its applications. We then state the isogeny problems in a more general form and discuss their computational hardnesses. Finally, we prove that the proposed scheme is secure in the presence of a quantum adversary under certain assumptions.

Mathematics Subject classification: 94A60, 14H52, 14K02

1. INTRODUCTION

Blind signature scheme is a protocol in which the *requester* requests the *signer* to sign a document without disclosing the contents of the document. In 1982, Chaum [8] proposed the first blind signature scheme. It is based on the *RSA problem* [27]. Since then a host of blind signature schemes and their variations have been proposed based on different hardness assumptions such as the Discrete Logarithm Problem (DLP), pairing-based problems and lattice-based problems [7, 26, 37]. However, all the known blind signature schemes suffer from a common drawback that they are not secure in the presence of a quantum adversary. The blind signatures by Chaum [8], Camenisch et al. [7] and Zhang and Kim [37] are not quantum secure due to the polynomial time quantum algorithm by Shor [31] for solving integer factorization and discrete logarithms. The lattice-based blind signature by Rückert [26] uses Fiat-Shamir paradigm [12] which is not secure in the quantum random oracle model as shown in [10].

Blind signature provides both anonymity and authentication. Hence it is used in the privacy-preserving protocols such as e-cash and e-voting. However, the signer has neither any control on the content of the document nor on the way the signature is used. Therefore, there is a crucial need to give a certain degree of control to the signer. One possible way is to let the signer

Key words and phrases. isogeny, supersingular elliptic curve, undeniable blind signature, post-quantum cryptography.

This work is supported by Indian Space Research Organization (ISRO) through Sponsored Research (RESPOND) programme.

and the requester agree on a part of the message (e.g., certain metadata about the specific message). This can be achieved through the technique introduced by Abe and Fujisaki [1].

Alternatively, one could let the signer decide who can verify the signature. This will keep unauthorized verifiers at bay and provide a certain control on the way the signature is used. The *Undeniable Signature* scheme introduced by Chaum and van Antwerpen [9] precisely has the said requirement. In an undeniable signature scheme the signer can decide who can verify the signature.

So, it seems desirable to have a scheme that would provide anonymity and controlled verification satisfying the properties of both blind signature and undeniable signature. Such a scheme can be devised but not obvious. In 1996, Sakurai and Yamane [29] have come up with an undeniable blind signature scheme based on the DLP. Their technique is also applicable for blinding the RSA based undeniable signature described in [9]. However, their scheme is not quantum secure either.

In this paper, we propose a new undeniable blind signature scheme based on the hardnesses of *isogeny problems* over supersingular elliptic curves. The isogeny problems for supersingular curves (details in Section 5) do not have any subexponential quantum algorithm. Hence, our scheme is quantum resistant.

Sun et al. [33] have used the hardness of isogeny problems for constructing *designated verifier signature* scheme. Jao and Soukharev [19] have proposed an isogeny-based undeniable signature. We extend Jao-Soukharev scheme into an Undeniable Blind Signature scheme.

To sum up, the main contributions of this paper are:

- (1) The concept of an UBSS seems to have been first mentioned in the work of Sakurai and Yamane [29]. However, to the best of our knowledge, it has never been formally defined in the literature till date. In this paper, we make such an attempt and give a formal definition of UBSS. We also study its properties including its strengths and weaknesses.
- (2) In [20], Jao and Venkatesan, speculate the use of hardness assumptions related to isogeny problems in constructing blind signature. We confirm this speculation by constructing an undeniable blind signature scheme.
- (3) The existing isogeny-based schemes [11, 19], including the current work, use primes of special forms that depend on a given set of small primes. Therefore, we state isogeny problems in their general form. These definitions can be used for the construction of any isogeny-based cryptographic scheme.

The rest of the paper is organized as follows. In Section 2, a formal definition of a UBSS is given and its properties as well as the possible attacks are studied. In Section 3 a brief and relevant mathematical background

about isogenies between supersingular elliptic curves is provided. Section 4 describes the proposed UBSS in detail. In Section 5, we state the isogeny problems in their general form and discuss related hardness assumptions. The security of the proposed scheme is proved in Section 6. We conclude in Section 7.

2. UNDENIABLE BLIND SIGNATURE: DEFINITION AND PROPERTIES

2.1. Formal Definition. One would expect that a UBSS combines the properties of undeniable signature scheme and blind signature scheme. This means that UBSS would offer anonymity of the message origination and controlled verification of the signature. We have not found any definition that would fulfill both the requirements. Taking inspiration from Rogaway [28], ours is an attempt to provide a definition for UBSS.

Definition 2.1 (Undeniable Blind Signature Scheme). An interactive signature scheme given by the tuple

$$UBSS = (\text{KeyGen}, \text{Blind}, \text{Sign}, \text{Unblind}, \text{Check}, \mathcal{CON}, \mathcal{DIS})$$

is said to be undeniable blind signature scheme if it satisfies the following:

- (1) The randomized *key generation algorithm* KeyGen takes as input a security parameter 1^λ and outputs a pair of keys (vk, sk) which are called the *verification key* and the *secret key* respectively. This is written as $(vk, sk) \leftarrow \text{KeyGen}(1^\lambda)$
- (2) The randomized *blinding algorithm* Blind takes as input a message m and outputs a blinded message m' , denoted as $m' \leftarrow {}_r\text{Blind}(m)$ where r is the random choice made by the algorithm.
- (3) The randomized or deterministic *signing algorithm* Sign takes as input a secret key sk and a message m . It outputs a signature σ , denoted $\sigma \leftarrow \text{Sign}_{sk}(m)$
- (4) The deterministic *unblinding algorithm* Unblind takes as input a blinded signature σ' and a random choice r . It outputs an unblinded signature σ , to be denoted by $\sigma := \text{Unblind}_r(\sigma')$
- (5) The deterministic *checking algorithm* Check takes as input a message m , a signature σ and the key pair (vk, sk) . It outputs a bit b with $b = 1$ meaning *valid* and $b = 0$ meaning *invalid*. This is written as $b := \text{Check}_{(vk, sk)}(m, \sigma)$
- (6) The *confirmation protocol*, π_{con} initiated by the signer, assures the verifier that the signature is indeed valid.
- (7) The *disavowal protocol*, π_{dis} also initiated by the signer, assures the verifier that the signature is not valid.

It is required that, for every key pair (vk, sk) output by $\text{KeyGen}(1^\lambda)$, every m in the message space, and every random choice r made by Blind , the following holds:

$$\text{Check}_{(vk, sk)}(m, \text{Unblind}_r(\text{Sign}_{sk}({}_r\text{Blind}(m)))) = 1$$

Additionally, if the signature algorithm is deterministic, we may also assume that the effect of *blinding-signing-unblinding* on a message is same as directly signing the message. In the above notation, this means

$$\text{Unblind}_r(\text{Sign}_{sk}(r\text{Blind}(m))) = \text{Sign}_{sk}(m)$$

2.2. Working of UBSS. We will now run through the protocol to illustrate the role of the different algorithms in the definition. The illustration also makes it clear when these algorithms are run and by whom.

At first the signer chooses a security parameter λ and runs $\text{KeyGen}(1^\lambda)$ to obtain the key pair (vk, sk) . The signing key sk is kept secret and the verification key vk is published by the signer. Let m be the message which the requester wishes to communicate anonymously. The requester first creates a blinded version m' of m by running the algorithm $\text{Blind}(m)$. Let r be the random choice made by the algorithm Blind . The requester then sends m' along with his identity Id_R . The signer verifies the requester's identity (see Remark 2.2) and runs Sign_{sk} on m' to obtain the blinded signature σ' . After receiving σ' from the signer, the requester unblinds it by using the algorithm Unblind and the same random choice r made by Blind . The requester then sends the original message m and the unblinded signature σ to the concerned party.

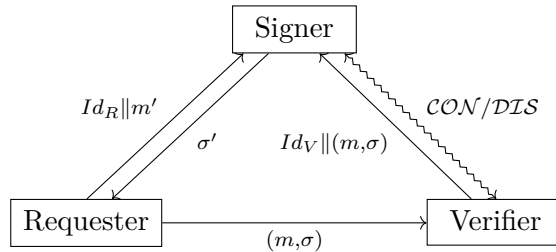


FIGURE 1. Illustration of the flow of information in an Undeniable Blind Signature Protocol

Any party who wishes to verify the signature sends the message-signature pair (m, σ) along with his identity Id_V to the signer. The signer verifies the identity of the verifier (see Remark 2.2). If Id_V is not the identity of an authorized verifier, then the signer simply ignores; otherwise, runs the algorithm Check . If Check returns *valid* then the signer initiates the confirmation protocol CON ; otherwise initiates the disavowal protocol DIS . Figure 1 gives the flow of information in the UBSS.

Remark 2.2. We intentionally do not specify how the signer verifies the identity of the requester and the verifier. It is the problem that can be best dealt with *mutual authentication* which can be done in one of the many ways [4, 5, 15], all of which are *quantum secure*.

2.3. Properties. The UBSS is desired to have the following three security properties viz., *unforgeability*, *blindness* and *invisibility*. The above properties are elaborated and their formal definitions are given below.

Unforgeability. As with any signature scheme, we require that the UBSS is unforgeable. The strongest notion of unforgeability is obtained when the adversary is allowed to corrupt both the requester and the verifier. The strongest notion of unforgeability for a UBSS is given here. The UBSS must be unforgeable against one-more forgery i.e., a requester who has received signatures for t messages (where t is polynomially bound by the security parameter), should not be able to output $t + 1$ distinct message-signature pairs even after collaborating with the verifier. This notion of unforgeability is formalized by the following security game:

- (1) The challenger runs $\text{KeyGen}(1^\lambda)$ to obtain the key pair (vk, pk) and gives the verification key vk to \mathcal{A} .
- (2) \mathcal{A} is allowed to make polynomially many queries to the signing oracle on chosen messages or any of their blinded versions adaptively and arbitrarily interleaved.
- (3) \mathcal{A} is also allowed to submit message-signature pairs (m, σ) to the confirmation/disavowal oracle. If (m, σ) is valid (resp. invalid), then the oracle engages in confirmation (resp. disavowal) protocol with the adversary.
- (4) After making t queries to the signing oracle, \mathcal{A} outputs t' distinct pairs (m_i, σ_i) such that

$$\text{Check}_{(vk, sk)}(m_i, \sigma_i) = 1$$

Definition 2.3 (Unforgeability). Let \mathcal{UBSS} be a given undeniable blind signature scheme as in Definition 2.1. We say that the \mathcal{UBSS} is *unforgeable* if $\Pr[t' > t]$ is negligible for any probabilistic polynomial-time (PPT) adversary \mathcal{A} in the above game.

Blindness. The blindness property is essential for preserving the anonymity of the message content originator. The signer should not be able to relate the message-signature pair and associated blinded versions. Although blindness theoretically ensures anonymity, to what degree the requester remains anonymous can vary in the real world as discussed in [2]. The strongest notion of blindness is obtained when the adversary is allowed to corrupt both the signer and verifier. Since the verification happens collaboratively with the signer, we allow the signer to view the signature after unblinding it. Incidentally, the existing definition of blindness for blind signature already accounts for this. Excepting notation, we consider the following security game as described by Schröder and Unruh in [30, Sec.3 Defn.4].

- (1) The adversary \mathcal{A} runs $\text{KeyGen}(1^\lambda)$ and generates a key pair (vk, sk) .
- (2) \mathcal{A} then chooses two messages m_0 and m_1 and gives them to the challenger.

- (3) The challenger chooses a random bit b hidden from \mathcal{A} and reorders the messages as (m_b, m_{b-1}) .
- (4) The challenger then blinds the two messages; $m'_b \leftarrow_{r_1} \text{Blind}(m_b)$ and $m'_{b-1} \leftarrow_{r_2} \text{Blind}(m_{b-1})$.
- (5) \mathcal{A} engages in signing the blinded versions m'_b and m'_{b-1} . If signing requires multiple interactions, then \mathcal{A} may engage parallelly and arbitrarily interleaved.
- (6) The challenger receives the blinded signatures σ'_b and σ'_{b-1} and unblinds them; $\sigma_b := \text{Unblind}_{r_1}(\sigma'_b)$ and $\sigma_{b-1} := \text{Unblind}_{r_2}(\sigma'_{b-1})$.
- (7) The challenger then sends σ_b and σ_{b-1} to \mathcal{A} .
- (8) At the end of the attack game, \mathcal{A} outputs a guess bit b' .

Definition 2.4 (Blindness). We say that the $UBSS$ has *blindness* property if $|\Pr[b' = b] - 1/2|$ is negligible for any PPT adversary \mathcal{A} in the above game.

Invisibility. A verifier should be able to accept (or reject) a signature only with the signer's cooperation via the confirmation (or disavowal) protocol and not otherwise. This notion is formalized by the following security game between a challenger \mathcal{C} and an adversary \mathcal{A} . This definition is based on the work of Kurosawa and Heng [24, Sec. 3 Defn. 5 p. 39].

- (1) The challenger runs $\text{KeyGen}(1^\lambda)$ to obtain the key pair (vk, pk) and gives the verification key vk to \mathcal{A} .
- (2) \mathcal{A} is permitted to issue a series of signing queries for messages m_i and their blinded versions to the signing oracle adaptively and receives signatures σ_i .
- (3) \mathcal{A} is also allowed to submit message-signature pairs (m, σ) to the confirmation/disavowal oracle. If (m, σ) is valid (resp. invalid), then the oracle engages in confirmation (resp. disavowal) protocol with the adversary.
- (4) At some point, \mathcal{A} chooses a message m^* and sends it to the challenger.
- (5) \mathcal{C} chooses a random bit b . If $b = 1$, \mathcal{C} runs $\sigma^* \leftarrow \text{Sign}_{sk}(m^*)$, otherwise, \mathcal{C} chooses a random value for σ^* from the signature space. \mathcal{C} returns σ^* to \mathcal{A} .
- (6) \mathcal{A} performs some signing queries again (see Remark 2.6).
- (7) \mathcal{A} can also perform some queries to the confirmation/disavowal oracle but not allowed to query the challenge (m^*, σ^*) .
- (8) At the end of the attack game, \mathcal{A} outputs a guess bit b' .

Definition 2.5 (Invisibility). We say that the $UBSS$ is *invisible* against full attack if $|\Pr[b' = b] - 1/2|$ is negligible for any PPT adversary \mathcal{A} in the above game.

Remark 2.6. If the signing algorithm is deterministic, we do not allow the adversary \mathcal{A} to query m^* or any of its blinded versions to the signing oracle.

2.4. Attacks: Blindness vs. Invisibility. A couple of attacks which exploit *blindness* property and *invisibility* property are demonstrated here. We

show that all the existing schemes [17, 23] that combine these two requirements are vulnerable to the following attacks. At the end of the section, some suggestions to choose the appropriate model and suitable application are made in order that the system is secure.

The restriction in Remark 2.6 is a standard practice. However it seems rather forced. Suppose that the signing algorithm is deterministic and adversary \mathcal{A} queries for a signature on a blinded version of m^* . If the UBSS is blind, then it is impossible for the signer to distinguish m^* from any of the previously signed messages. Hence, \mathcal{A} can easily guess b and the signature is visible for the requester without actually engaging in the confirmation/disavowal protocol.

Suppose the signer does not conform to his inputs, say a different key pair (vk^*, sk^*) is used instead of (vk, sk) for signing all the messages from a particular requester. If the UBSS is invisible, it is impossible for the requester to know that the signer has used a different key pair. During the verification of a message-signature pair (m, σ) , if $\text{Check}_{(vk, sk)}(m, \sigma)$ returns *invalid*, and $\text{Check}_{(vk^*, sk^*)}(m, \sigma)$ returns *valid*, then the signer can trace the origin of the message m . Thus, compromising the anonymity of the content originator. The signer seamlessly continues with the disavowal protocol. This anomaly could be seen as an advantage. Suppose the requester becomes aware that the signer has used a different key pair for signing. The requester may choose to give up the anonymity of the message to expose the signer. The signatures can be used as an evidence against the signer.

One way to circumvent the above attacks is to allow the requester to be a valid verifier. This makes the signatures visible to the requester and empowers the requester to check whether the signer has used the correct input.

The definition of UBSS is decoupled from the actual security model and the applications. While anonymity and invisibility appear to be conflicting goals, by choosing an appropriate model (like *semi-honest model* [16]), UBSS can be very useful in certain applications. For example, in the case of e-cash, one may consider the bank as a semi-honest signer. For security reasons, the bank could decide to verify signatures only for its customers. Then the bank should use UBSS instead of blind signatures.

Another example where the UBSS becomes a natural choice is *Anonymous Feedback System*. Suppose the chief organizer of an event wishes to take anonymous feedback from the participants. It should be done such that (i) only the participants should be able to give the feedback anonymously and (ii) only the organizing committee should be able to verify the authenticity of the feedback. The participants who give feedback request for a blind signature from the chief organizer. After obtaining the signature, the participants send the feedback along with the signature to the organizing committee. The committee members then verify the signature with the chief organizer. *E-voting* can be considered as a special case of anonymous feedback system.

This completes our discussion on the definition of the UBSS. In the next few sections, we give an example of a UBSS using the isogeny-based hardness assumptions.

3. MATHEMATICAL BACKGROUND

This section briefly provides some necessary mathematical background. For further details, the reader is referred to [32] for mathematical, [13] for cryptographic, [11] for algorithmic aspects and the citations thereof.

Let \mathbb{F}_q be the finite field (up to isomorphism) of characteristic p and cardinality q . It is a well known fact that two elliptic curves are isomorphic over an algebraic closure of \mathbb{F}_q if and only if they have the same j -invariant. Also, given two elliptic curves, the isomorphism between them can be efficiently computed [14]. An elliptic curve E/\mathbb{F}_q is said to be *supersingular* if $\#E(\mathbb{F}_q) \equiv 1 \pmod{p}$. For equivalent definitions kindly refer [18, Ch. 13 Sec. 3 p. 259].

Isogenies. A homomorphism between two groups is a map that preserves the group structure. The *kernel* of a homomorphism is the subset of elements whose image is the identity. An *isogeny* is a group homomorphism between two elliptic curves with a *finite* kernel. Let $\phi : E_1 \rightarrow E_2$ be an isogeny between two elliptic curves E_1 and E_2 . Thus $\phi(O_{E_1}) = O_{E_2}$ and ϕ can be written as

$$\phi(x, y) = \left(\frac{f_1(x, y)}{g_1(x, y)}, \frac{f_2(x, y)}{g_2(x, y)} \right),$$

where f_1, f_2, g_1, g_2 are polynomials in two variables x, y with co-efficients in \mathbb{F}_q . The *degree* of the isogeny ϕ , $\deg \phi = \max\{\deg f_1, \deg f_2\}$. An isogeny ϕ is said to be *separable* if $\deg \phi = \#\ker \phi$. An isogeny of degree ℓ is often referred to as an ℓ -isogeny. For any ℓ -isogeny $\phi : E_1 \rightarrow E_2$, there exists an ℓ -isogeny $\hat{\phi} : E_2 \rightarrow E_1$, called the *dual* of ϕ , such that $\phi \circ \hat{\phi} = \hat{\phi} \circ \phi = [\ell]$ where $[\ell]$ is a multiplication-by- ℓ map. Two elliptic curves E_1 and E_2 are said to be ℓ -isogenous if there exists an ℓ -isogeny ϕ between them. Tate's isogeny theorem [34] says that E_1 and E_2 are isogenous over \mathbb{F}_q if and only if $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$. An isogeny is uniquely identified (up to isomorphism) by its kernel. Any generator of the kernel will produce a unique isogeny up to isomorphism via Vélu's formulae [36]. In our work we will be considering only supersingular elliptic curves and separable isogenies with cyclic kernels.

Isogeny Graph. An ℓ -isogeny graph is a graph in which the nodes are represented by isomorphism classes of elliptic curves. There is an edge from E_1 to E_2 in the ℓ -isogeny graph if there is an ℓ -isogeny from E_1 to E_2 . The isogeny graph is undirected due to the existence of dual isogenies. The ℓ -isogeny graph of supersingular curves is connected [25]. Given two random nodes in the isogeny graph finding a path of fixed length is hard. This hardness is used for constructing isogeny-based cryptosystems, explained in detail in Section 5.

4. A NEW UNDENIABLE BLIND SIGNATURE SCHEME BASED ON ISOGENIES

In this section, we describe a new undeniable blind signature scheme based computing an isogeny between two supersingular elliptic curves over a finite field \mathbb{F}_q . We borrow the notation as in the paper of Jao and Soukharev [19].

4.1. Public parameters. Choose a prime p of the form $p = \ell_A^{e_A} \ell_M^{e_M} \ell_C^{e_C} \ell_R^{e_R} \cdot f \pm 1$. Generate a random supersingular elliptic curve E_0 defined over the field \mathbb{F}_{p^2} . Such a curve can be efficiently found using the algorithm by Bröker et al. [6, Sec. 4 Alg. 4.1 p. 106]. Choose base points $\{P_A, Q_A\}$, $\{P_M, Q_M\}$, $\{P_C, Q_C\}$ and $\{P_R, Q_R\}$ that generate $E_0[\ell_A^{e_A}]$, $E_0[\ell_M^{e_M}]$, $E_0[\ell_C^{e_C}]$ and $E_0[\ell_R^{e_R}]$ respectively. Choose a hash function $H : \{0, 1\}^* \rightarrow \frac{\mathbb{Z}}{\ell_M^{e_M} \mathbb{Z}}$.

4.2. KeyGen. The signer generates two random numbers $m_A, n_A \in \mathbb{Z}/\ell_A^{e_A} \mathbb{Z}$. Computes the curve $E_A = E_0 / \langle K_A \rangle$ where $K_A = [m_A]P_A + [n_A]Q_A$ is the generator of the kernel of the isogeny $\phi_A : E_0 \rightarrow E_A$. The signer also computes $\phi_A(P_C)$ and $\phi_A(Q_C)$.

Public Key: $E_A, \phi_A(P_C), \phi_A(Q_C)$

Private Key: m_A, n_A, K_A

$$E_0 \xrightarrow{\phi_A} E_A$$

FIGURE 2. The isogeny ϕ_A computed during the key generation phase.

4.3. Blind. Let M be the message for which the signature is required. Let $h = H(M)$. Compute the isogeny ϕ_M and the curve

$$E_M = \frac{E_0}{\langle P_M + [h]Q_M \rangle}$$

The image points $\phi_M(P_A)$, $\phi_M(Q_A)$, $\phi_M(P_C)$, $\phi_M(Q_C)$, $\phi_M(P_R)$ and $\phi_M(Q_R)$ are also computed. Now this message curve E_M has to be blinded. Choose a random $r \in \frac{\mathbb{Z}}{\ell_R^{e_R} \mathbb{Z}}$ which is hidden from the signer. Compute the isogeny $\phi_{M, RM}$ and the curve

$$E_{RM} = \frac{E_M}{\langle \phi_M(P_R) + [r]\phi_M(Q_R) \rangle}$$

E_{RM} is the blinded curve on which the signer will sign. The blinding process is illustrated in Figure 3.

Before sending the curve E_{RM} for signing, one has to compute the dual isogeny $\hat{\phi}_{M, RM}$, so that unblinding is possible. To do that, first we need to find a point $K \in E_M[\ell_R^{e_R}]$ of order $\ell_R^{e_R}$ such that $K \notin \text{Ker} \phi_{M, RM}$, say $K = \phi_M(Q_R)$. Compute the image point $\phi_{M, RM}(K) \in E_{RM}$. The isogeny with kernel $\langle \phi_{M, RM}(K) \rangle$ is the dual isogeny $\hat{\phi}_{M, RM}$.

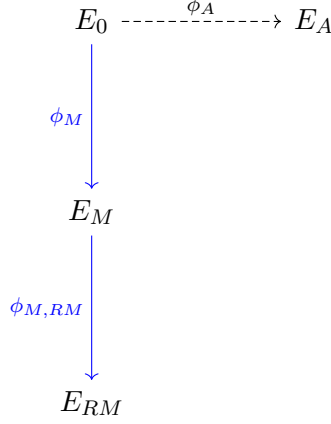


FIGURE 3. The isogenies ϕ_M and $\phi_{M,RM}$ computed while blinding the message. The dashed arrow is the isogeny unknown to the requester.

Remark 4.1. Strictly speaking, this will not be the dual of $\phi_{M,RM}$ because this isogeny will lead to a curve which is isomorphic to E_M . Since isomorphic curves represent the same node in the isogeny graph, this isogeny maps back to the same node. By the abuse of notation, we denote it as $\hat{\phi}_{M,RM}$.

Now, choose basis $\{P'_R, Q'_R\} \in E_{RM}$ that generate $E_{RM}[\ell_R^{e_R}]$. Compute $m, n \in \frac{\mathbb{Z}}{\ell_R^{e_R}}$ such that

$$\phi_{M,RM}(K) = [m]P'_R + [n]Q'_R$$

This amounts to solving extended discrete logarithm problem on E_{RM} . Since E_{RM} is isogenous to E_0 , by Tate's theorem [34], we have

$$\#E_{RM}(\mathbb{F}_{p^2}) = \#E_0(\mathbb{F}_{p^2})$$

Hence E_{RM} is a curve of smooth order. Therefore, m, n can be found efficiently using generalized Pohlig-Hellman algorithm given by Teske in [35, Sec. 4 Alg. 4.1 p. 529]. The masked curve E_{RM} along with the points

$$P'_A = \phi_{M,RM}(\phi_M(P_A))$$

$$Q'_A = \phi_{M,RM}(\phi_M(Q_A))$$

$$P'_C = \phi_{M,RM}(\phi_M(P_C))$$

$$Q'_C = \phi_{M,RM}(\phi_M(Q_C))$$

P'_R and Q'_R (all belonging to E_{RM}) is sent to the signer.

4.4. **Sign.** The signer computes the curve

$$E_{ARM} = \frac{E_{RM}}{\langle [m_A]P'_A + [n_A]Q'_A \rangle}$$

The signer also computes the image points $\phi_{RM,ARM}(P'_C)$, $\phi_{RM,ARM}(Q'_C)$, $\phi_{RM,ARM}(P'_R)$ and $\phi_{RM,ARM}(Q'_R)$, and sends all the computed values to the user.

$$\begin{array}{ccc}
 E_0 & \xrightarrow{\phi_A} & E_A \\
 \downarrow \phi_M & & \\
 E_M & & \\
 \downarrow \phi_{M,RM} & & \\
 E_{RM} & \xrightarrow{\phi_{RM,ARM}} & E_{ARM}
 \end{array}$$

FIGURE 4. The isogeny $\phi_{RM,ARM}$ computed for signing the blinded message. The dashed arrows are the isogenies unknown to the signer.

4.5. **Unblind.** The requester computes the isogeny $\hat{\phi}_{AM,ARM}$ and the curve

$$E_{AM} = \frac{E_{ARM}}{\langle [m]\phi_{RM,ARM}(P'_R) + [n]\phi_{RM,ARM}(Q'_R) \rangle}$$

The requester also computes the points

$$P_S = \hat{\phi}_{AM,ARM}(\phi_{RM,ARM}(P'_C))$$

$$Q_S = \hat{\phi}_{AM,ARM}(\phi_{RM,ARM}(Q'_C))$$

The signature $\sigma = \{E_{AM}, P_S, Q_S\}$.

4.6. **Check.** At the end of Unblind algorithm, the signature curve generated by our scheme is isomorphic to Jao-Soukharev signature curve. Hence the signature verification can be done in the same way as in Jao-Soukharev signature. When a message M and signature σ is submitted for verification, the signer first checks whether the square (E_0, E_A, E_{AM}, E_M) in Figure 6 commutes. If it does, then the signer initiates the confirmation protocol \mathcal{CON} , initiates the disavowal protocol \mathcal{DIS} . The confirmation and disavowal protocols are same as in [19].

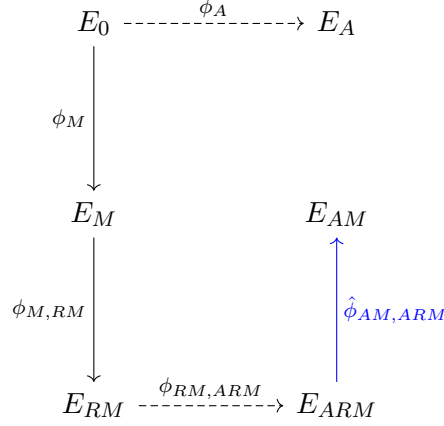


FIGURE 5. The isogeny $\hat{\phi}_{AM,ARM}$ computed while unblinding the signature. The dashed arrows are the isogenies unknown to the requester.

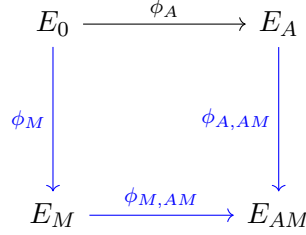


FIGURE 6. The isogenies ϕ_M , $\phi_{M,AM}$, $\phi_{A,AM}$ are computed to check whether the given signature E_{AM} is valid.

Remark 4.2. Strictly speaking, the effect of *blinding-signing-unblinding* is not the same as directly signing the message. The action of an isogeny followed by the action of its dual is equivalent to multiplication-by-degree map [32, III.6.2a p. 83]. Hence, the points P_S and Q_S will have a factor of $\ell_R^{e_R}$ multiplied to them when compared to the Jao-Soukharev signature. But then, this factor is relatively prime to their order $\ell_C^{e_C}$. It would not affect the signature verification since both the pairs generate the same kernel.

The prime used in our work is different from the primes already used in the literature [11, 19] for constructing isogeny-based cryptographic primitives. This motivates us to give generalized statements and hardness assumptions for isogeny-problems. We review them in the next section.

5. ISOGENY PROBLEMS REVISITED

The current work uses the prime p of the form $p = \ell_A^{e_A} \ell_M^{e_M} \ell_C^{e_C} \ell_R^{e_R} \cdot f \pm 1$ which has not been used so far in the literature. The security of the isogeny-based schemes depend on the size of the corresponding torsion subgroup. Hence, such a choice for the prime does not have any security implications so long as the torsion groups are large enough.

Let p be a prime of the form $p = f \cdot \prod_{i=1}^N \ell_i^{e_i} \pm 1$ where ℓ_i are distinct small primes, e_i are positive integers and $f \geq 1$ is a small cofactor. Let E_0 be a supersingular elliptic curve defined over \mathbb{F}_{p^2} and having order $(p \mp 1)^2$. For each $1 \leq i \leq N$, let $\{P_i, Q_i\}$ be an arbitrarily chosen basis of $E_0[\ell_i^{e_i}]$. The above informations form the global parameters.

Problem 5.1 (Decisional Supersingular Isogeny (DSSI) problem). Given the global parameters and another curve E' defined over \mathbb{F}_{p^2} such that $\#E_0(\mathbb{F}_{p^2}) = \#E'(\mathbb{F}_{p^2})$, decide whether E' is $\ell_i^{e_i}$ -isogenous to E_0 for a specified $1 \leq i \leq N$.

For a fixed but arbitrary $1 \leq i \leq N$, let $\phi_i : E_0 \rightarrow E_i$ be an isogeny whose kernel is $\langle [m_i]P_i + [n_i]Q_i \rangle$ where $m_i, n_i \in \mathbb{Z}/\ell_i^{e_i}\mathbb{Z}$ are chosen randomly and not both divisible by ℓ_i .

Problem 5.2 (Computational Supersingular Isogeny (CSSI) problem). Given the global parameters, the curve E_i and the points $\phi_i(P_j), \phi_i(Q_j)$ for all $j = 1, 2, \dots, N, j \neq i$, find a generator of $\langle [m_i]P_i + [n_i]Q_i \rangle$.

5.1. DSSI and CSSI Assumptions. The DSSI and CSSI assumptions are the assumptions that DSSI and CSSI problems are hard to solve for any $1 \leq i \leq N$. This notion is formalized in this section.

DSSI Assumption. The DSSI assumption says that the following two probability distributions are *computationally indistinguishable* for all i :

- $(E, E/\langle R \rangle)$ where $R \in E$ is a random point of order $\ell_i^{e_i}$.
- (E, E') where E'/\mathbb{F}_{p^2} is a random curve such that $\#E(\mathbb{F}_{p^2}) = \#E'(\mathbb{F}_{p^2})$.

Let λ be the security parameter. Let \mathcal{G} be a (possibly randomized) polynomial-time algorithm that, on input 1^λ , outputs the global parameters described above. Let us denote the set of all the global parameters by \mathbb{G} .

Definition 5.3. We say that the DSSI problem is *hard* relative to \mathcal{G} if $\forall 1 \leq i \leq N$ and for all bounded quantum polynomial-time algorithms \mathcal{A} , the quantity

$$|\Pr[\mathcal{A}(\mathbb{G}, E, E/\langle R \rangle) = 1] - \Pr[\mathcal{A}(\mathbb{G}, E, E') = 1]|$$

is negligible and the probabilities in each case is taken over the experiment in which $\mathcal{G}(1^\lambda)$ outputs \mathbb{G} , $R \in E$ is a random point of order $\ell_i^{e_i}$ and E' is a random curve such that $\#E(\mathbb{F}_{p^2}) = \#E'(\mathbb{F}_{p^2})$.

CSSI Assumption. Consider the following experiment for a given parameter-generating algorithm \mathcal{G} , algorithm \mathcal{A} , and parameter λ :

The computational supersingular isogeny experiment $\text{CSSIso}_{\mathcal{A},\mathcal{G}}(\lambda)$:

- (1) Run $\mathcal{G}(1^\lambda)$ to obtain the global parameters $\mathbb{G} = (p, E_0, \ell_i, e_i, P_i, Q_i)$.
- (2) For a fixed $1 \leq i \leq N$, choose $m, n \leftarrow \mathbb{Z}/\ell_i^{e_i}$ not both divisible by ℓ_i and compute

$$E' \equiv \frac{E_0}{\langle [m]P_i + [n]Q_i \rangle}$$

- (3) \mathcal{A} is given \mathbb{G}, i, E' and outputs a point $R \in E_0$.
- (4) The output of the experiment is defined to be 1 if $E' \equiv \frac{E_0}{\langle R \rangle}$ and 0 otherwise.

Definition 5.4. We say that the CSSI problem is *hard* relative to \mathcal{G} if $\forall 1 \leq i \leq N$ and for all bounded quantum polynomial-time algorithms \mathcal{A} there exists a negligible function negl such that

$$\Pr[\text{CSSIso}_{\mathcal{A},\mathcal{G}}(\lambda) = 1] \leq \text{negl}(\lambda)$$

5.2. Hardness of CSSI and DSSI Assumptions. Since the DSSI and CSSI problems need to be hard for all values of i , it is expected that the parameter generating algorithm \mathcal{G} outputs the prime p such that the values $\ell_i^{e_i}$ are roughly of the same size for all i . Hence, we assume $\ell_i^{e_i} \approx \sqrt[3]{p}$. The generic attack for solving DSSI and CSSI problems that improve on exhaustive search involve solving the *claw problem* for the domain size $\ell_i^{e_i/2}$. The optimal complexity for the above black-box claw attack using a quantum computer is $O(\ell_i^{e_i/3}) = O(\sqrt[3]{p})$. Suppose $\lambda = \log p$, then the complexity of the attack is $O(2^{\lambda/3N})$ which is clearly exponential in λ . Kohel et al. [22] have given a probabilistic algorithm for solving the quaternion analog of CSSI problem. However, translating it to CSSI problem is not known to be efficient. The quantum algorithm by Biasse et al. [3] yields a subexponential attack if the base curve is defined over \mathbb{F}_p . There is no known subexponential attack if the base curve is not defined over \mathbb{F}_p .

5.3. Other Isogeny Problems. There have been several other variants of DSSI and CSSI problems whose hardness have been assumed to build the cryptographic primitives. We present only those that are relevant to the current work. For a complete list, we refer the reader to [19, Sec. 5]. Henceforth in the rest of the paper, for the sake of simplicity, we follow the notation as in Section 4.

Problem 5.5 (Decisional Supersingular Product (DSSP) problem). Given an isogeny $\phi : E_0 \rightarrow E_3$ of degree $\ell_i^{e_i}$ and a tuple sampled with probability $1/2$ from one of the following two distributions:

- (E_1, E_2, ϕ') where the product $E_1 \times E_2$ is chosen at random among those $\ell_j^{e_j}$ -isogenous ($i \neq j$) to $E_0 \times E_3$, and where $\phi' : E_1 \rightarrow E_2$ is an isogeny of degree $\ell_i^{e_i}$, and
- (E_1, E_2, ϕ') where E_1 is chosen at random among the curves having the same cardinality as E_0 , and $\phi' : E_1 \rightarrow E_2$ is a random isogeny of degree $\ell_i^{e_i}$,

determine from which distribution the tuple is sampled.

Problem 5.6 (Modified Supersingular Computational Diffie-Hellman (MSSCDH) problem). Given E_A , E_M and $\ker(\phi_M)$, determine E_{AM} .

Problem 5.7 (One-sided Modified Supersingular Computational Diffie-Hellman (q -OMSSCDH) problem). For a fixed E_A and given oracle access of at most q times to MSSCDH for any set of inputs E_A , E_{M_i} , $\ker(\phi_{M_i})$, ($1 \leq i \leq q$). Solve MSSCDH for E_A , E_M and $\ker(\phi_M)$ where $E_M \neq E_{M_i} \forall i$.

Problem 5.8 (Modified Supersingular Decisional Diffie-Hellman (MSSDDH) problem). Given E_A , E_M , E_C and $\ker(\phi_M)$, decide whether $E_C \equiv E_{AM}$.

Problem 5.9 (One-sided Modified Supersingular Decisional Diffie-Hellman (q -OMSSDDH) problem). For a fixed E_A and given oracle access of at most q times to MSSCDH oracle for any set of inputs E_A , E_{M_i} , $\ker(\phi_{M_i})$, ($1 \leq i \leq q$). Solve MSSDDH for E_A , E_M , E_C and $\ker(\phi_M)$ where $E_M \neq E_{M_i} \forall i$.

Signing Oracle. Given any supersingular elliptic curve $\mathcal{E}/\mathbb{F}_{p^2}$ of order $(\ell_A^{e_A} \ell_M^{e_M} \ell_C^{e_C} \ell_R^{e_R})^2$ and points $P, Q \in \mathcal{E}$ both of order $\ell_A^{e_A}$, the signing oracle outputs the curve \mathcal{E}_A such that

$$\mathcal{E}_A \equiv \frac{\mathcal{E}}{[m_A]P + [n_A]Q}$$

where $m_A, n_A \in \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$ form the private key.

Problem 5.10 (One-More Supersingular Computational Diffie-Hellman (1MSSCDH) problem). After making q queries to the signing oracle, output at least $q + 1$ distinct pairs of curves $\{E_{M_i}, E_{AM_i}\}$ where E_{M_i} are $\ell_M^{e_M}$ -isogenous to E_0 and $\{E_A, E_{M_i}, E_{AM_i}\}$ is a Diffie-Hellman tuple for each $1 \leq i \leq t$.

6. SECURITY OF THE PROPOSED CONSTRUCTION

In this section, we prove that our UBSS has unforgeability, blindness and invisibility.

6.1. Unforgeability. The challenger chooses a security parameter and generates the secret key m_A, n_A . The corresponding public key $E_A, \phi_A(P_C), \phi_A(Q_C)$ is given to the adversary \mathcal{A} . \mathcal{A} then issues a series of at most q signing queries to the challenger for the messages m_i ($1 \leq i \leq q$). Let E_{M_i} and E_{AM_i} be the corresponding message curves and signatures respectively. \mathcal{A} is allowed to submit the message-signature pairs (m, E_{AM}) to the signer for verification. If the signature is correct then the signer engages in confirmation protocol otherwise initiates disavowal protocol. At some point adversary then outputs q' message-signature pairs (m_j, E_{AM_j}) . The adversary wins the game if $q' > q$.

Theorem 6.1 (Unforgeability). *If the DSSP and 1MSSCDH assumptions hold, then the proposed UBSS is unforgeable.*

Proof. Suppose there exists an adversary \mathcal{A} that forges the proposed UBSS. Without any loss of generality we may assume that \mathcal{A} issued exactly q signing queries and output exactly $q + 1$ valid message-signature pairs. The confirmation and disavowal protocols are shown to be zero-knowledge in [19, Sec. 7] provided DSSP is hard to solve. Hence we may further assume that \mathcal{A} does not have access to the confirmation/disavowal oracle at all. But then \mathcal{A} in turn solves 1MSSCDH problem. \square

Remark 6.2. Since the signature for a message m obtained at the end of the proposed UBSS protocol is the Jao-Soukharev signature for m , we also need to assume that solving q -OMSSCDH problem is hard. This is omitted in the statement of Theorem 6.1 as 1MSSCDH assumption is stronger than q -OMSSCDH assumption.

6.2. Blindness. To prove that the proposed signature scheme has blindness property, the security game described in [21, Sec. 2 p. 156] is used. The adversary \mathcal{A} is given the security parameter. \mathcal{A} generates the secret key m_A, n_A and the corresponding public key $E_A, \phi_A(P_C), \phi_A(Q_C)$. The adversary outputs two messages $\{m_0, m_1\}$. The same two messages are ordered as $\{m_b, m_{1-b}\}$ according to a random bit b which is hidden from \mathcal{A} . Then \mathcal{A} engages in two parallel interactive protocols, possibly with two different users. If the users output the corresponding signatures, then \mathcal{A} is also given E_{AM_0} and E_{AM_1} . \mathcal{A} 's goal is to guess the value of the bit b and the blindness property requires that such a guess is negligibly close to $\frac{1}{2}$.

Theorem 6.3 (Blindness). *If the DSSP is hard to solve, then the proposed UBSS has the blindness property.*

Proof. Given $E_{M_0}, E_{M_1}, E_{RM_b}, E_{RM_{1-b}}, E_{AM_0}, E_{AM_1}$ the goal of the adversary \mathcal{A} is to figure out the value of the bit b . Note that \mathcal{A} also has the knowledge of the isogenies $\phi_{s_0} : E_{M_0} \rightarrow E_{AM_0}$, $\phi_{s_1} : E_{M_1} \rightarrow E_{AM_1}$, $\phi'_{s_b} : E_{RM_b} \rightarrow E_{ARM_b}$ and $\phi'_{s_{1-b}} : E_{RM_{1-b}} \rightarrow E_{ARM_{1-b}}$. To decide whether $b = 0$ or $b = 1$ is equivalent to deciding whether, $E_{RM_b} \times E_{ARM_b}$ is ℓ_R^{eR} -isogenous to $E_{M_0} \times E_{AM_0}$ or not. Further, this essentially amounts to solving DSSP on the inputs $(E_{M_0}, E_{AM_0}, \phi_{s_0})$ and $(E_{RM_b}, E_{ARM_b}, \phi'_{s_b})$. \square

6.3. Invisibility. The challenger chooses a security parameter and generates the secret key m_A, n_A . The corresponding public key $E_A, \phi_A(P_C), \phi_A(Q_C)$ is given to the adversary \mathcal{A} . \mathcal{A} then issues a series of at most q signing queries to the challenger for the messages m_i . Let E_{M_i} and E_{AM_i} be the corresponding message curves and signatures respectively. \mathcal{A} is allowed to query E_{M_i} and any of its blinded versions to the signing oracle. \mathcal{A} is also allowed to submit the message-signature pairs (m_j, E_{AM_j}) to the confirmation/disavowal protocols. At some point \mathcal{A} outputs a message m^* . The challenger chooses a random bit b . If $b = 0$, the challenger replies with the correct signature E_{AM^*} otherwise chooses a random curve E_R with $\#E_R(\mathbb{F}_{p^2}) = \#E_0(\mathbb{F}_{p^2})$. Let E_{AM} be the signature for the message m . According to the definition

of invisibility, the message curve E_M and none of its blinded versions are allowed to query the signing oracle.

Theorem 6.4 (Invisibility). *If the DSSP and q -OMSSDDH assumptions hold, then the proposed UBSS is invisible.*

Proof. If the DSSP assumption holds, then the confirmation and disavowal protocols are shown to be zero-knowledge [19, Sec.7] in the presence of a quantum adversary. Hence we may assume that the adversary \mathcal{A} does not have access to confirmation/disavowal oracle. Instead, the access is given to an oracle which on querying (m, E) outputs valid or invalid depending on whether E is a valid signature for m or not. Further, \mathcal{A} is not allowed to query the signing oracle for the curve E_M or any of its blinded versions. Hence showing the invisibility of our signature scheme is equivalent to showing that the Jao-Soukharev signature is invisible. The reader may refer [19, Sec.6] for the proof of invisibility. \square

7. CONCLUSION

We give a formal definition of UBSS as well as modified definitions of blindness, invisibility and unforgeability; concepts that are key in defining UBSS. As we mentioned earlier, though the concept of UBSS is not new and has been mentioned in Sakurai and Yamane [29], this is the first time a formal definition has been given. We also show that blindness and invisibility play against each other. This affects the specifics of how UBSS can be used for the application at hand. We then described a new UBSS based on the isogeny problem for supersingular elliptic curves. We also give the generalized statements of isogeny problems. This makes it convenient for constructions of isogeny-based cryptographic primitives. We finally prove that our UBSS has the desired properties under the assumptions that DSSP, OMSSDDH and 1MSSCDH are hard to solve.

8. ACKNOWLEDGEMENTS

The first author thanks Vijay M. Patankar for guidance, helpful discussions and a careful first reading of the manuscript. He also thanks David Jao for suggestions (i) to formalize the definition of UBSS (ii) to give a careful thought to its applications (iii) to state the isogeny problems in a general form and (iv) to improve the exposition.

REFERENCES

- [1] Masayuki Abe and Eiichiro Fujisaki. How to Date Blind Signatures. In *Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security: Advances in Cryptology, ASIACRYPT '96*, pages 244–251, London, UK, 1996. Springer-Verlag.
- [2] Anonymous. To Reveal or Not to Reveal: A Theoretical Model of Anonymous Communication. *Communication Theory*, 8(4):381–407, 1998.

- [3] Jean-François Biasse, David Jao, and Anirudh Sankar. A Quantum Algorithm for Computing Isogenies between Supersingular Elliptic Curves. In Willi Meier and Debdeep Mukhopadhyay, editors, *Progress in Cryptology – INDOCRYPT 2014*, volume 8885 of *Lecture Notes in Computer Science*, pages 428–442. Springer International Publishing, 2014.
- [4] Dan Boneh and Mark Zhandry. Quantum-Secure Message Authentication Codes. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology – EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Computer Science*, pages 592–608. Springer Berlin Heidelberg, 2013.
- [5] Dan Boneh and Mark Zhandry. Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013*, volume 8043 of *Lecture Notes in Computer Science*, pages 361–379. Springer Berlin Heidelberg, 2013.
- [6] Reinier Bröker, Denis Charles, and Kristin Lauter. Evaluating Large Degree Isogenies and Applications to Pairing Based Cryptography. In Steven D. Galbraith and Kenneth G. Paterson, editors, *Pairing-Based Cryptography – Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, pages 100–112. Springer Berlin Heidelberg, 2008.
- [7] Jan L. Camenisch, Jean-Marc Piveteau, and Markus A. Stadler. Blind signatures based on the discrete logarithm problem. In Alfredo De Santis, editor, *Advances in Cryptology – EUROCRYPT’94*, volume 950 of *Lecture Notes in Computer Science*, pages 428–432. Springer Berlin Heidelberg, 1995.
- [8] David Chaum. Blind Signatures for Untraceable Payments. In David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, *Advances in Cryptology*, pages 199–203. Springer US, 1983.
- [9] David Chaum and Hans van Antwerpen. Undeniable Signatures. In Gilles Brassard, editor, *Advances in Cryptology - CRYPTO’ 89 Proceedings*, volume 435 of *Lecture Notes in Computer Science*, pages 212–216. Springer New York, 1990.
- [10] Özgür Dagdelen, Marc Fischlin, and Tommaso Gagliardoni. The Fiat–Shamir Transformation in a Quantum World. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology - ASIACRYPT 2013*, volume 8270 of *Lecture Notes in Computer Science*, pages 62–81. Springer Berlin Heidelberg, 2013.
- [11] Luca De Feo, David Jao, and Jerome Plut. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3):209–247, June 2014.
- [12] Amos Fiat and Adi Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In *Proceedings on Advances in cryptology—CRYPTO ’86*, pages 186–194, London, UK, 1987. Springer-Verlag.
- [13] Steven Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, April 2012.
- [14] Steven D. Galbraith. Constructing Isogenies Between Elliptic Curves Over Finite Fields. *LMS J. Comput. Math*, 2:118–138, 1999.
- [15] Sebastianus A. Goorden, Marcel Horstmann, Allard P. Mosk, Boris Škorić, and Pepijn W. H. Pinkse. Quantum-secure authentication of a physical unclonable key. *Optica*, 1(6):421–424, Dec 2014.
- [16] Carmit Hazay and Yehuda Lindell. Semi-honest Adversaries. In *Efficient Secure Two-Party Protocols*, Information Security and Cryptography, pages 53–80. Springer Berlin Heidelberg, 2010.
- [17] Zhenjie Huang, Zhixiong Chen, and Yumin Wang. Convertible undeniable partially blind signatures. In *Advanced Information Networking and Applications, 2005. AINA 2005. 19th International Conference on*, volume 1, pages 609–614 vol.1, March 2005.
- [18] Dale Husemoller. *Elliptic Curves*. Springer, 2nd edition, 2004.

- [19] David Jao and Vladimir Soukharev. Isogeny-Based Quantum-Resistant Undeniable Signatures. In Michele Mosca, editor, *Post-Quantum Cryptography*, volume 8772 of *Lecture Notes in Computer Science*, pages 160–179. Springer International Publishing, 2014.
- [20] D.Y. Jao and R. Venkatesan. Use of isogenies for design of cryptosystems, December 24 2013. CA Patent 2,483,486.
- [21] Ari Juels, Michael Luby, and Rafail Ostrovsky. Security of Blind Digital Signatures (Extended Abstract). In *CRYPTO '97: Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology*, pages 150–164. Springer-Verlag, 1997.
- [22] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion ℓ -isogeny path problem. *LMS Journal of Computation and Mathematics*, 17:418–432, 2014.
- [23] A. Koide, R. Tso, and E. Okamoto. Convertible Undeniable Partially Blind Signature from Bilinear Pairings. In *Embedded and Ubiquitous Computing, 2008. EUC '08. IEEE/IFIP International Conference on*, volume 2, pages 77–82, Dec 2008.
- [24] Kaoru Kurosawa and Swee-Huay Heng. Relations Among Security Notions for Undeniable Signature Schemes. In Roberto De Prisco and Moti Yung, editors, *Security and Cryptography for Networks*, volume 4116 of *Lecture Notes in Computer Science*, pages 34–48. Springer Berlin Heidelberg, 2006.
- [25] Arnold K. Pizer. Ramanujan graphs and Hecke operators. *Bull. Amer. Math. Soc. (N.S.)*, 23(1):127–137, 07 1990.
- [26] Markus Rückert. Lattice-Based Blind Signatures. In Masayuki Abe, editor, *Advances in Cryptology - ASIACRYPT 2010*, volume 6477 of *Lecture Notes in Computer Science*, pages 413–430. Springer Berlin Heidelberg, 2010.
- [27] Ronald L Rivest and Jr. Kaliski, Burt. RSA Problem. In Henk C.A. van Tilborg and Sushil Jajodia, editors, *Encyclopedia of Cryptography and Security*, pages 1065–1069. Springer US, 2011.
- [28] Phillip Rogaway. On the Role Definitions in and Beyond Cryptography. In Michael J. Maher, editor, *Advances in Computer Science - ASIAN 2004. Higher-Level Decision Making*, volume 3321 of *Lecture Notes in Computer Science*, pages 13–32. Springer Berlin Heidelberg, 2005.
- [29] Kouichi Sakurai and Yoshinori Yamane. Blind decoding, blind undeniable signatures, and their applications to privacy protection. In Ross Anderson, editor, *Information Hiding*, volume 1174 of *Lecture Notes in Computer Science*, pages 257–264. Springer Berlin Heidelberg, 1996.
- [30] Dominique Schröder and Dominique Unruh. Security of Blind Signatures Revisited. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *Public Key Cryptography – PKC 2012*, volume 7293 of *Lecture Notes in Computer Science*, pages 662–679. Springer Berlin Heidelberg, 2012.
- [31] P. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Review*, 41(2):303–332, 1999.
- [32] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2nd edition, June 2009.
- [33] 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, Sept 2012.
- [34] John Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones mathematicae*, 2(2):134–144, 1966.
- [35] Edlyn Teske. The Pohlig–Hellman Method Generalized for Group Structure Computation. *Journal of Symbolic Computation*, 27(6):521 – 534, 1999.
- [36] Jacques Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.

- [37] Fangguo Zhang and Kwangjo Kim. ID-Based Blind Signature and Ring Signature from Pairings. In Yuliang Zheng, editor, *Advances in Cryptology — ASIACRYPT 2002*, volume 2501 of *Lecture Notes in Computer Science*, pages 533–547. Springer Berlin Heidelberg, 2002.

SRI SATHYA SAI INSTITUTE OF HIGHER LEARNING, PUTTAPARTHI, INDIA 515134.
E-mail address: `srinathms@sssihl.edu.in`

SRI SATHYA SAI INSTITUTE OF HIGHER LEARNING, PUTTAPARTHI, INDIA 515134.
E-mail address: `vchandrasedkaran@sssihl.edu.in`