Filomat 36:10 (2022), 3249–3258
https://doi.org/10.2298/FIL2210249E

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

An Isogeny-based Quantum-Resistant Secret Sharing Scheme

Khadijeh Eslami[a], Mojtaba Bahramian[a]

[a] *Department of Pure Mathematics, Faculty of Mathematical Sciences, University of Kashan, Kashan, Iran*

Abstract. In a secret sharing scheme, a secret is distributed among several participants in such a way that only any authorized subset of participants is able to recover the secret. So far, the security of many secret sharing schemes has been based on the hardness of some mathematical problems, such as discrete logarithm and factorization. These problems can be solved in polynomial time using Shor's algorithm for a quantum computer. In this paper, we propose an efficient multi-secret sharing scheme based on the hardness of computing isogenies between supersingular elliptic curves. The proposed scheme is based on De Feo and Jao key exchange protocol. We prove that our scheme is secure under computational assumptions in which there is no known efficient quantum algorithm.

1. Introduction

Secret sharing is a safe technique to protect the secrets with numerous applications in cryptography, visual cryptography, secret key agreement, threshold encryption, etc. In 1979, the first (t, n)-threshold secret sharing schemes were introduced by Blakley and Shamir independently. Blakley's scheme is based on the linear projective geometry, while the other is based on Lagrange Interpolation. In a (t, n)-threshold secret sharing scheme, an authority called dealer distributes a secret as shares amongst n participants in such a way that any group of minimum size t can pool their secret shadows and easily reconstruct the secret, while no groups having at most $t-1$ members can learn anything about the secret. A multi-secret sharing scheme is a scheme in which several secrets are shared among participants, and any predefined subset of them can reconstruct all the secrets. The first multi-secret sharing scheme was introduced by He and Dawson [29] in 1994, and was improved in several studies such as [8, 9, 19, 26–28, 34].

So far, the security of many secret sharing schemes has been based on the hardness of some mathematical problems, such as integer factorization and the discrete logarithmic problem [16, 38, 41]. Both of these problems can be solved in polynomial time using Shor's algorithm by a quantum computer [40]. Hence, using the elliptic curve discrete logarithm problem is not suitable for constructing quantum-resistant cryptosystems. There are several candidates for postquantum cryptography, some of them are lattice-based cryptography [25, 36], code-based cryptography [2, 7, 35], multi-variate cryptography [5, 50], hash-based cryptography [6, 15] and recently isogeny-based cryptography [30]. The latter is appealing for the relatively small key sizes compared to other post-quantum candidates.
Ordinary and supersingular elliptic curves are two different types of these curves. The first cryptosystem

2020 *Mathematics Subject Classification*. Primary 11G07; Secondary 14K02, 11T71
Keywords. Secret Sharing, Elliptic Curves, Isogenies, Quantum-Resistant Public-Key Cryptosystems.
Received: 03 October 2019; Accepted: 15 August 2022
Communicated by Predrag Stanimirović
This research was in part supported by the University of Kashan under grant number 682460/013.
Email addresses: kh.eslami@grad.kashanu.ac.ir (Khadijeh Eslami), bahramianh@kashanu.ac.ir (Mojtaba Bahramian)

based on the hardness of computing isogenies between elliptic curves was independently proposed by Couveignes and Stolbunov [14, 44]. Both of them used ordinary elliptic curves, that is based on commutative ring theory. Childs et al. observed that the problem of finding an isogeny between two ordinary curves E_1, E_2 defined over $\mathbb{F}_q$ and having the same endomorphism ring could be reduced to the problem of finding a subgroup of a dihedral group. They present a subexponential-time quantum algorithm to break this system [11]. The idea of supersingular isogeny protocols is based on the isogeny for ordinary elliptic curves. The case of the ordinary elliptic curves is based on commutative ring theory and the supersingular case is non-commutative, so it is a suitable candidate for a post-quantum-secure system.

Cryptosystems based on supersingular isogenies are very important in post-quantum cryptography. The supersingular curve protocols were first designed in a hash function construction by Charles, Lauter, and Goren [10]. Jao and De Feo presented a cryptosystem based on the difficulty of constructing isogenies between supersingular elliptic curves, which is still infeasible against the known quantum attacks [30]. Further cryptosystems in the supersingular elliptic curve isogenies were proposed by Jao, De Feo and Plut [22]. Key exchange protocol, zero-knowledge proof of identity and public key encryption proposed by Jao, and De Feo are prominent examples for protocols based on the hardness of computing isogenies between supersingular elliptic curves.

In 2016, Galbraith, Petit, and Silva proposed signature schemes based on supersingular elliptic curve isogenies [24], and in 2017, R. Azarderakhsh et al. presented a quantum-resistant digital signature scheme based on supersingular isogeny problems with very small key sizes [51]. In 2018 Kim et al. [32] proposed formulas for computing 3 and 4-isogenies on twisted Edwards curves, which can be applied in isogeny based cryptography. An undeniable signature scheme based on supersingular elliptic curve isogenies was presented by Jao et al. [31]. Srinath et al. proposed an undeniable blind signature scheme based on isogenies between supersingular elliptic curves [39].

This article proposed a new verifiable (t, n)-threshold multi-secret sharing scheme based on supersingular elliptic curve isogenies. There are two methods to construct isogeny between elliptic curves, that were introduced by Velu [48] and Kohel [33]. Velu's formula gives an isogeny for a given elliptic curve and a finite subgroup as the kernel, and in Kohel's method the isogeny can be computed from the kernel polynomial. In this work, we use Velu's formula to construct isogenies and Jao-De Feo's key exchange protocol to publish the shares.

The rest of the paper is organized as follows: In Section 2 a brief mathematical background about elliptic curves and isogenies between supersingular elliptic curves is provided. Section 3 describes the proposed secret sharing scheme in detail. In Sections 4 and 5 we state the isogeny problems and discuss about the security of our proposed scheme.

2. Preliminaries

2.1. Elliptic Curves

Here, we provide a mathematical background on elliptic curves that we need throughout the rest of the paper. For further details, the reader is referred to [42, 49]. An elliptic curve E defined over a field K is a nonsingular plane curve with the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

where $a_1, a_2, a_3, a_4, a_6 \in K$. If the characteristic of K is not 2 or 3, the equation (1) can be written in the short form $y^2 = x^3 + ax + b$, where $a, b \in K$. If O is the point at infinity, the set of K-rational points of E, defined by

$$E(K) = \{(x, y) \in K^2 : y^2 = x^3 + ax + b\} \cup \{O\}$$

forms an abelian group with O as the identity element. The n-torsion subgroup of $E(\bar{K})$, denoted by $E[n]$ is the set of points $P \in E(\bar{K})$ for which $nP = O$.

If the characteristic of K is zero or does not divide n, then $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$, and if the characteristic of K is $p > 0$ and $n = p^r n'$ with $\gcd(p, n') = 1$, then $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_{n'}$ or $\mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'}$. If $q = p^r$, where p is a prime, an elliptic curve E over the field $\mathbb{F}_q$ is said to be supersingular if $E[p] = \mathcal{O}$, otherwise we say that E is ordinary. For the elliptic curve $E : y^2 = x^3 + ax + b$, we define quantities $\Delta = 4a^3 + 27b^2$ and $j(E) = 1728\frac{4a^3}{4a^3+27b^2}$, that are called the discriminant of the Weierstrass equation and the j-invariant of the elliptic curve, respectively. The elliptic curves E_1/K and E_2/K are isomorphic over $\bar{K}$, if and only if they have the same j-invariant.

2.2. Isogenies

Now, we briefly introduce some basic concepts on the isogeny of elliptic curves, for more details on the mathematical foundations, the reader can refer to [22, 42]. Let p be a prime, $q = p^r$, and let E_1 and E_2 be two elliptic curves defined over the field $\mathbb{F}_q$. An isogeny $\varphi : E_1 \to E_2$ is a non-constant algebraic morphism defined over $\mathbb{F}_q$ of the form

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

satisfying $\varphi(\mathcal{O}) = \mathcal{O}$. We say the elliptic curves E_1 and E_2 are isogenous, if there exists an isogeny $\varphi : E_1 \to E_2$. Two isogenous elliptic curves are either both supersingular or both ordinary. The degree of an isogeny φ, denoted by $\deg(\varphi)$, is the degree of φ as a morphism. The isogeny $\varphi : E_1 \to E_2$ is separable if the function field extension $\mathbb{F}_q(E_1)/\varphi^*(\mathbb{F}_q(E_2))$ is separable. In this case we have $\deg(\varphi) = \#\ker(\varphi)$ [42, III.4.10(c)]. An isogeny φ is called ℓ-isogeny when the degree of φ is ℓ. Notice that, the number of ℓ-isogenies, whose domain is E_1 is equal to the number of distinct subgroups of E_1 of order ℓ. Tate's theorem states that two elliptic curves E_1 and E_2 are isogenous over a finite field $\mathbb{F}_q$, if and only if $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$ [46]. For each ℓ- isogeny $\varphi : E_1 \to E_2$, there exists a unique isogeny $\widehat{\varphi} : E_2 \to E_1$, which satisfies $\widehat{\varphi} \circ \varphi = \varphi \circ \widehat{\varphi} = [l]$. The isogeny $\widehat{\varphi}$ is called the dual isogeny of φ. For a given pair of isogenies $\varphi : E_1 \to E_2$ and $\psi : E_2 \to E_1$ satisfying $\psi \circ \varphi = 1_{E_1}$ and $\varphi \circ \psi = 1_{E_2}$, we say that φ and ψ are isomorphism.

For a prime p, every supersingular elliptic curve defined over $\bar{\mathbb{F}}_p$ is isomorphic to a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$, so that we can consider supersingular elliptic curves all defined over $\mathbb{F}_{p^2}$. Therefore, there is only a finite number of supersingular elliptic curves up to isomorphism. For every prime $\ell \nmid p$, there exist exactly $\ell+1$ cyclic subgroups of order ℓ in the torsion subgroup $E[\ell]$, each one corresponding to a different isogeny. Any generator of the kernel K will define a unique isogeny up to isomorphism via Velu's formula [42, III.4.12]. For this reason, the codomain E_2 of the isogeny φ is often denoted by the quotient E_1/K. In this paper, we will only consider separable supersingular isogenies, also, all kernel of the isogenies that will be used are cyclic groups. Hence, knowledge of the kernel, knowledge of any generator of the kernel, and knowledge of the isogeny are equivalent. There are some both easy and hard computational problems associated to isogenies. We state a problem from each as follows:

Explicit isogeny: Let E_1 and E_2 be two d-isogenous elliptic curves over a finite field. Find an isogeny $\varphi : E_1 \to E_2$ of degree d.

Isogeny path: Let E_1 and E_2 be two elliptic curves over a finite field K, with the property that $\#E_1(K) = \#E_2(K)$. Find an isogeny $\varphi : E_1 \to E_2$ of smooth degree.

The first algorithm to solve the explicit isogeny problem is proposed by Elkies with complexity $O(d^3)$ [18], and then some other algorithms are proposed with complexity $O(d^2)$ [12, 13, 20, 21]. The isogeny path problem is one of the hard problems in isogeny-based cryptography, in which only exponential time algorithms are known in general [23].

2.3. Key Exchange Protocol

Here, we review Jao-De Feo's key exchange protocol using isogenies on supersingular elliptic curves.

2.3.1. Parameter Generation

Let p be a prime number of the form $p = \ell_A^{e_A}\ell_B^{e_B} f \pm 1$, where ℓ_A and ℓ_B are distinct small primes such that $\ell_A^{e_A} \approx \ell_B^{e_B} \approx 2^\lambda$, e_A and e_B are positive integers, and f is some cofactor. Also, fix a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ such that $\#E(\mathbb{F}_{p^2})$ has order divisible by $(\ell_A^{e_A}\ell_B^{e_B})^2$. Fix points $P_A, Q_A \in E[\ell_A^{e_A}]$ and $P_B, Q_B \in E[\ell_B^{e_B}]$ such that $E[\ell_A^{e_A}] = \langle P_A, Q_A\rangle$ and $E[\ell_B^{e_B}] = \langle P_B, Q_B\rangle$. In this protocol the parameters E, P_A, Q_A, P_B, Q_B are public. We refer the reader to [4, 22] for the details on the computations.

2.3.2. Key Exchange

The supersingular isogeny Diffie-Hellman (SIDH) key exchange protocol works as follows: Alice chooses two random elements $m_A, n_A \in \mathbb{Z}_{\ell_A^{e_A}}$, not both divisible by ℓ_A. She computes an isogeny $\varphi_A : E \to E_A$ with kernel $K_A = \langle [m_A]P_A + [n_A]Q_A \rangle$ and publishes $\{E_A, \varphi_A(P_B), \varphi_A(Q_B)\}$. Similarly, Bob chooses $m_B, n_B \in \mathbb{Z}_{\ell_B^{e_B}}$, computes an isogeny $\varphi_B : E \to E_B$ having kernel $K_B = \langle [m_B]P_B + [n_B]Q_B \rangle$ and publishes $\{E_B, \varphi_B(P_A), \varphi_B(Q_A)\}$. To compute the shared key, Alice computes an isogeny $\varphi'_A : E_B \to E_{AB}$ having kernel equal to $\langle [m_A]\varphi_B(P_A) + [n_A]\varphi_B(Q_A) \rangle = \langle \varphi_B(K_A) \rangle$. Similarly, Bob computes an isogeny $\varphi'_B : E_A \to E'_{AB}$ with kernel $\langle [m_B]\varphi_A(P_B) + [n_B]\varphi_A(Q_B) \rangle = \langle \varphi_A(K_B) \rangle$. Notice that, elliptic curve equations E_{AB} and E'_{AB} are not likely to be the same, but the curves are isomorphic and so $j(E_{AB}) = j(E'_{AB})$. Therefore, the common j-invariant is the secret shared key.

Remark 2.1. *To computing $\langle [m_A]P_A + [n_A]Q_A \rangle$ we can assume that m_A is invertible modulo ℓ_A, in which case, $\langle [m_A]P_A + [n_A]Q_A \rangle = \langle P_A + [m_A^{-1} n_A]Q_A \rangle$. The generator $T = P_A + [m_A^{-1} n_A]Q_A$ can be computed by a standard double-and-add method, and it needs half the effort of computing $[m_A]P_A + [n_A]Q_A$ [1, 17, 43].*

3. Proposed Scheme

This section introduces a verifiable (t, n)-threshold multi-secret sharing scheme using isogenies between supersingular elliptic curves. The security of the scheme is based on the difficulty of computing isogenies between supersingular elliptic curves, which is quantum-resistant [22]. We start with some basics about Jao-De Feo's key exchange protocol. In our scheme $U_1, U_2, \dots, U_n$ are all the participants and a dealer D shares the secrets $K_1, K_2, \dots, K_m$ among the participants in such a way that any group of t or more participants can together recover all the secrets, while no groups having at most $t-1$ members can learn anything about the secrets.

3.1. Initialization Phase

Let p be a prime of the form $p = \ell_D^{e_D}\ell_1^{e_1}\cdots\ell_n^{e_n} f \pm 1$, where $\ell_D, \ell_1, \cdots, \ell_n$ are distinct small primes, the exponents $e_D, e_1, \cdots, e_n$ are positive integers, and f is a small cofactor. Also, fix a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ such that the order group, $\#E(\mathbb{F}_{p^2})$, is divisible by $(\ell_D^{e_D}\ell_1^{e_1}\cdots\ell_n^{e_n})^2$. Fix points $P_D, Q_D \in E[\ell_D^{e_D}]$ and $P_i, Q_i \in E[\ell_i^{e_i}]$, such that $E[\ell_D^{e_D}] = \langle P_D, Q_D \rangle$ and $E[\ell_i^{e_i}] = \langle P_i, Q_i \rangle$ for $i = 1, \cdots, n$. The elliptic curve E and the points $P_D, Q_D, P_1, Q_1, \cdots, P_n, Q_n$ are public.

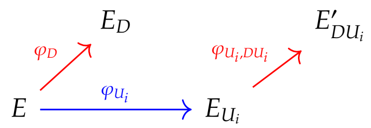
3.2. Points Sharing Phase

In this phase, the following steps are performed by the dealer and the participant U_i for $i = 1, \cdots, n$.

1. The dealer chooses two secret random integers $m_D, n_D \in \mathbb{Z}_{\ell_D^{e_D}}$, not both divisible by ℓ_D, and computes an isogeny $\varphi_D : E \to E_D$ with kernel generated by $K_D = \langle [m_D]P_D + [n_D]Q_D \rangle$. The dealer computes $\varphi_D(P_i)$ and $\varphi_D(Q_i)$, and publishes $E_D, \varphi_D(P_i)$ and $\varphi_D(Q_i)$.

2. Similarly, participant U_i chooses two secret random integers $m_i, n_i \in \mathbb{Z}_{\ell_i^{e_i}}$, not both divisible by ℓ_i, and computes an isogeny $\varphi_{U_i} : E \to E_{U_i}$ having kernel $K_i = \langle [m_i]P_i + [n_i]Q_i \rangle$. U_i computes $\varphi_{U_i}(P_D)$ and $\varphi_{U_i}(Q_D)$, then publishes these two points together with the curve E_{U_i}.

3. Upon receipt of E_{U_i} and $\varphi_{U_i}(P_D), \varphi_{U_i}(Q_D) \in E_{U_i}$ from U_i, the dealer computes the isogeny $\varphi_{U_i,DU_i} : E_{U_i} \to E'_{DU_i}$ with kernel generated by $\varphi_{U_i}(K_D)$ and calculates $j_i = j(E'_{DU_i})$.



4. The dealer considers the matrix

$$A = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & 2 & \dots & 2^{n+m-1} \\ \vdots & \vdots & & \vdots \\ 1 & n+m-t & \dots & (n+m-t)^{n+m-1} \end{bmatrix}$$

and the column vector $X = [j_1, \cdots, j_n, K_1, \cdots, K_m]^T$, and then computes and publishes the column vector

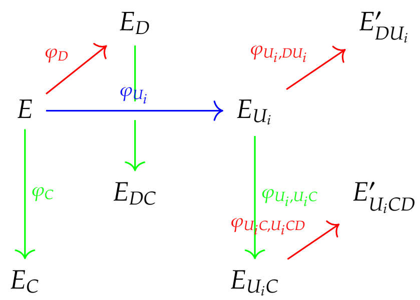
$$A \times X \quad = [I_1, \cdots, I_{n+m-t}]^T. \tag{2}$$

3.3. *Verification Phase*

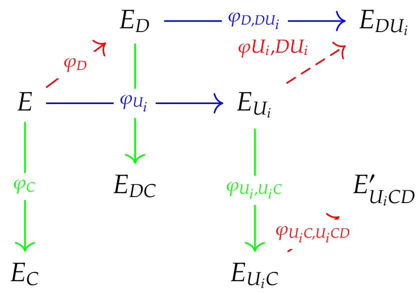
In this phase, we suppose that t distinct participants $U_1, \cdots, U_t$ want to reconstruct all the secrets by sending their shares to a combiner C, who is one of the participants. It is possible that a malicious participant provides a fake share to combiner. Therefore, upon receipt of the shares from participants, the combiner confirms them. When the combiner ensures that all the shares are valid, he reconstructs the secrets. In the process of creating secret shared key between the dealer and combiner, the points $\varphi_D(P_C)$ and $\varphi_D(Q_C)$ are published by the dealer. Also, participant U_i publishes the points $\varphi_{U_i}(P_C)$ and $\varphi_{U_i}(Q_C)$ to generate secret shared key between the combiner and U_i.
The steps of the shares verification are expressed as follows:

- Combiner C uses elliptic curve E_{U_i} and auxiliary points $\varphi_{U_i}(P_C)$ and $\varphi_{U_i}(Q_C)$ to compute the isogeny $\varphi_{U_i,U_iC} : E_{U_i} \to E_{U_iC}$ having kernel generated by $\varphi_{U_i}(K_C) = [m_C]\varphi_{U_i}(P_C) + [n_C]\varphi_{U_i}(Q_C)$. Then he publishes $\varphi_{U_i,U_iC}(\varphi_{U_i}(P_D))$, $\varphi_{U_i,U_iC}(\varphi_{U_i}(Q_D))$ and E_{U_iC}.

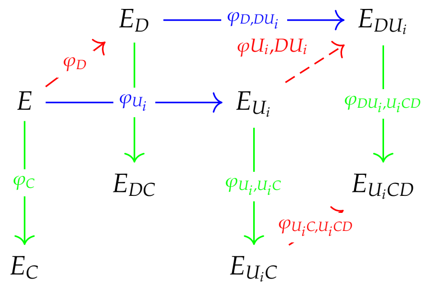
- The dealer by using public parameters $\varphi_{U_i,U_iC}(\varphi_{U_i}(P_D))$, $\varphi_{U_i,U_iC}(\varphi_{U_i}(Q_D))$ and E_{U_iC}, computes the isogeny $\varphi_{U_iC,U_iCD} : E_{U_iC} \to E'_{U_iCD}$ having kernel generated by $\varphi_{U_i,U_iC}(\varphi_{U_i}(K_D)) = [m_D]\varphi_{U_i,U_iC}(\varphi_{U_i}(P_D)) + [n_D]\varphi_{U_i,U_iC}(\varphi_{U_i}(Q_D))$, and sends E'_{U_iCD} to the combiner.



- Participant U_i computes the isogeny $\varphi_{D,DU_i} : E_D \to E_{DU_i}$ having kernel equal to $\langle \varphi_D(K_{U_i}) \rangle = \langle [m_i]\varphi_D(P_i) + [n_i]\varphi_D(Q_i) \rangle$ using the auxiliary points $\varphi_D(P_i), \varphi_D(Q_i)$. Participant U_i sends E_{DU_i} to the combiner, and publishes the points $\varphi_{D,DU_i}(\varphi_D(P_C))$ and $\varphi_{D,DU_i}(\varphi_D(Q_C))$.



- The combiner having the elliptic curve E_{DU_i} and the auxiliary points $\varphi_{D,DU_i}(\varphi_D(P_C))$ and $\varphi_{D,DU_i}(\varphi_D(Q_C))$, computes the isogeny $\varphi_{DU_i,U_iCD} : E_{DU_i} \to E_{U_iCD}$ with kernel generated by $\varphi_{D,DU_i}(\varphi_D(K_C)) = [m_C]\varphi_{D,DU_i}(\varphi_D(P_C))+ [n_C]\varphi_{D,DU_i}(\varphi_D(Q_C))$.



- The combiner accepts E_{DU_i}, if $j(E'_{U_iCD}) = j(E_{U_iCD})$. Otherwise, he will realize at least one of the curves E_{DU_i} or E'_{U_iCD} is fake and he stops the reconstruction phase.

3.4. Secrets Reconstruction Phase

Clearly, Eq. (2) is a system of $(m + n - t)$ linear equations in $m + n$ unknowns. We suppose that t distinct participants $U_1, \cdots, U_t$ want to reconstruct the secrets. Upon receipt of E_{iD} from U_i, the combiner confirms the share and computes $j_i = j(E_{DU_i})$. Hence, t unknowns of the Eq. (2) are disclosed and the other $(m+n-t)$ variables, especially $K_1, \cdots, K_m$, can be obtained by solving the system of equations in the Eq. (2).

Remark 3.1. *The dealer and the participant U_i compute the elliptic curve equations E'_{DU_i} and E_{DU_i} respectively. These two curves are not exactly the same, but they are isomorphic and so $j(E_{DU_i}) = j(E'_{DU_i})$.*

4. Isogeny Problems

As before, we use the prime of the form $p = l_D^{e_D} l_1^{e_1} \cdots l_n^{e_n} f \pm 1$ where l_D and l_i's are distinct small primes, e_D and e_i's are positive integers and f is some small integer cofactor. Let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$, having order $(p \mp 1)^2 = l_D^{2e_D} l_1^{2e_1} \cdots l_n^{2e_n} f^2$. Let $\{P_D, Q_D\}$ be a generating set for $E[l_D^{e_D}]$ and $\{P_i, Q_i\}$ be a set of generators of $E[l_i^{e_i}]$ for $i = 1, \cdots, n$. We assume that all of the above information is public. In the following, we present some hard problems related to supersingular elliptic curves [30, 31, 39].

Problem 4.1 (Decisional Supersingular Isogeny (DSSI) problem). *Given the above public parameters and another supersingular elliptic curve E' defined over $\mathbb{F}_{p^2}$ such that $\#E(\mathbb{F}_{p^2}) = \#E'(\mathbb{F}_{p^2})$, decide whether E' is $l_i^{e_i}$-isogenous to E for some $1 \le i \le n$.*

In the following problems, we suppose that $\varphi_D : E \to E_D$ is an isogeny with kernel generated by $[m_D]P_D + [n_D]Q_D$, where $m_D, n_D \in \mathbb{Z}_{l_D{}^{e_D}}$ are chosen at random and m_D, n_D are not both divisible by l_D, also $\varphi_i : E \to E_i$ is an isogeny whose kernel is $\langle [m_i]P_i + [n_i]Q_i \rangle$, where $m_i, n_i \in \mathbb{Z}_{l_i{}^{e_i}}$ are chosen at random and m_i, n_i are not both divisible by l_i.

Problem 4.2 (Computational Supersingular Isogeny (CSSI) problem). *Given the public parameters, the curve E_i and the image points $\varphi_i(P_D), \varphi_i(Q_D)$, find a generator of $\langle [m_i]P_i + [n_i]Q_i \rangle$.*

There are several variants of DSSI and CSSI problems based on the difficulty of computing isogenies between supersingular elliptic curves. Here, we present the ones we need in our scheme. For more information, see [31].

Problem 4.3 (Supersingular Computational Diffie-Hellman (SSCDH) problem). *Given the curves E_i, E_D and the points $\varphi_i(P_D), \varphi_i(Q_D), \varphi_D(P_i)$ and $\varphi_D(Q_i)$, find the j-invariant of $E/\langle [m_i]P_i + [n_i]Q_i, [m_D]P_D + [n_D]Q_D \rangle$.*

Problem 4.4 (Supersingular Decision Diffie-Hellman (SSDDH) problem). *Given a tuple sampled with probability 1/2 from one of the following distributions:*

- *$(E_i, E_D, \varphi_i(P_D), \varphi_i(Q_D), \varphi_D(P_i), \varphi_D(Q_i), E_{iD})$, where $(E_i, E_D, \varphi_i(P_D), \varphi_i(Q_D), \varphi_D(P_i)$, and $\varphi_D(Q_i)$ are as above and*

$$E_{iD} \cong E/\langle [m_i]P_i + [n_i]Q_i, [m_D]P_D + [n_D]Q_D \rangle,$$

- *$(E_i, E_D, \varphi_i(P_D), \varphi_i(Q_D), \varphi_D(P_i), \varphi_D(Q_i), E_C)$, where $E_i, E_D, \varphi_i(P_D), \varphi_i(Q_D), \varphi_D(P_i)$, and $\varphi_D(Q_i)$ are as above and*

$$E_C \cong E/\langle [m'_i]P_i + [n'_i]Q_i, [m'_D]P_D + [n'_D]Q_D \rangle,$$

determine from which distribution the tuple is sampled.

Problem 4.5 (Modified Supersingular Computational Diffie-Hellman (MSSCDH) problem). *With the notation used in the SSDDH problem, given E_i, E_D and ker(φ_D), compute E_{iD}.*

Problem 4.6 (Modified Supersingular Decisional Diffie-Hellman (MSSDDH) problem). *With the notation used in the SSDDH problem, given E_i, E_D, E_C and ker(φ_D), decide whether $E_C = E_{iD}$.*

5. Security

The problem of finding an isogeny between two isogenous supersingular elliptic curves over the finite field $\mathbb{F}_{p^2}$ was first considered by Galbraith [23], where he gave an algorithm that runs in time $O(p \log p)$. The fastest known algorithm to find an isogeny between two isogenous supersingular elliptic curves in general takes $O(\sqrt{p} \log^2 p)$ time [10]. The known attack against DSSI and CSSI problems are exponential. In order for the DSSI and CSSI problems to be hard, we need to choose the prime $p = l_D^{e_D} l_1^{e_1} \cdots l_n^{e_n} f \pm 1$ such that $l_D^{e_D} \approx l_1^{e_1} \approx \cdots \approx l_n^{e_n}$. Hence, we assume that $l_i^{e_i} \approx p^{1/n+1}$. The optimal complexity for solving these problems using a classical computer and a quantum computer is $O(l_i^{e_i/3}) = O(p^{1/(3n+3)})$ and $O(l_i^{e_i/2}) = O(p^{1/(2n+2)})$ respectively [45, 52].

In the proposed scheme, U_i's auxiliary points $\varphi_i(P_D)$ and $\varphi_i(Q_D)$ allow the dealer to compute isogeny φ_i on all the points in $E[l_D^{e_D}]$. This ability is needed to make the scheme feasible since the dealer needs to compute $\varphi_i(K_D)$. However, the participant U_i must never disclose $\varphi_i(P_i)$ or $\varphi_i(Q_i)$, since by revealing this information one can solve the extended discrete logarithm problem $m_i\varphi_i(P_i) + n_i\varphi_i(Q_i) = \varphi_i(m_iP_i + n_iQ_i) = 0$ in $E[l_i^{e_i}]$, easily [47]. It seems that there is no way to translate the values of φ_i on $E[l_D^{e_D}]$ into values on $E[l_i^{e_i}]$ [22].

Remark 5.1. *If the MSSCDH problem assumption holds, then any attacker cannot access computation E_{DU_i} and E'_{DU_i} using public parameters E_D, E_{U_i} and the points P_i, Q_i, P_D and Q_D.*

We prove that our scheme has the proper features for a secure secret sharing scheme. The proposed scheme does not need a secure channel and there is no limit in the number of secrets. Also, to identify the cheaters, the combiner can verify the shares the other participants sent. The security of the scheme is based on the hardness of the computational supersingular isogeny problem.

Theorem 5.2. *The dealer's private key* (m_D, n_D) *and the* U_i*'s private key* (m_i, n_i) *cannot be obtained from the public information.*

Proof. By contradiction proof, assume that there exists an algorithm such that an attacker can compute (m_D, n_D) for the given public parameters $E_D, \varphi_D(P_i), \varphi_(Q_i)$. Therefore, he can compute $[m_D]P_D + [n_D]Q_D$, which is a generator of $ker(\varphi_D)$. It means that the attacker can solve the CSSI problem using the algorithm, which is infeasible. Similarly, the other private key (m_i, n_i) cannot be obtained from the public information. □

The following theorem ensures that using a secure channel in the scheme to share parameters is not mandatory.

Theorem 5.3. *The proposed scheme does not require a secure channel.*

Proof. If an attacker wants to compute m_i and n_i from public parameters $\varphi_i(P_D)$, $\varphi_i(Q_D)$, $\varphi_i(P_C)$ and $\varphi_i(Q_C)$, he must solve a CSSI problem, which is infeasible. This ensures that no participant's shadow (m_i, n_i) can be obtained from public parameters. □

The theorem below illustrates the verifiability of the proposed scheme.

Theorem 5.4. *The shares provided by the participants in the reconstruction phase can be verified.*

Proof. Suppose that the participant U_i provides E_{U_iD}. During the reconstruction phase, the combiner can verify this share because, as mentioned before, elliptic curve equations E_{U_iCD} and E'_{U_iCD} are not exactly the same, but the curves are isomorphic and so $j(E'_{U_iCD}) = j(E_{U_iCD})$.
By Theorem 5.2, the secret shared key between the dealer and the combiner is secure and no attacker can obtain the dealer or combiner's private key. Similarly, the secret shared key between the combiner and participant U_i is secure. In the verification phase, the elliptic curves E_D, E_{U_i} and the points $\varphi_i(P_D), \varphi_i(Q_D), \varphi_D(P_i)$ and $\varphi_D(Q_i)$ are public. By SSCDH, it is infeasible to compute $j(E_{U_iD})$. Also, if the MSSCDH assumption holds, then any attacker does not have access to computation E_{DU_i} using public parameters E_D, E_{U_i} and the auxiliary points. Therefore, all steps of the verification phase are secure. □

Theorem 5.5. *In the proposed scheme, only qualified subsets of participants can recover the secrets.*

Proof. To this end, we prove that: i) any t or more participants can reconstruct all the secrets and ii) no group with less than t participants can compute any of the secrets.
i) Without loss of generality, we suppose that $\{U_i\}_{i=1}^t$ are the participants who want to reconstruct all the secrets by pooling their shares E_{U_iD}'s. Then, Eq. (2) is converted to a system of $m + n - t$ equations and $m + n - t$ unknowns with the invertible coefficients matrix

$$A' = \begin{bmatrix} 1 & \dots & 1 \\ 2^t & \dots & 2^{n+m-1} \\ \vdots & & \vdots \\ (n+m-t)^t & \dots & (n+m-t)^{n+m-1} \end{bmatrix}. \quad (3)$$

The determinant of A' can be calculated via $det(A') = ((n+m-t)!)^t \times det(A'')$, for some Vandermonde matrix A''. Hence, the secrets are obtained by computing the inverse matrix of A'.
ii) By contradiction proof, assume that this is the case. Then, Eq. (2) reduces to a system of $m + n - t$ equations and more than $m + n - t$ unknowns, which does not have a unique solution. □

References

[1] A. Antipa, D. Brown, R. Gallant, R. Lambert, R. Struik, S. Vanstone, Accelerated verification of ECDSA signatures, In Selected Areas in Cryptography 2005, volume 3897 of Lecture Notes in Computer Science, pages 307-318, Berlin, Heidelberg, 2006. Springer Berlin / Heidelberg.

[2] M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, D. Schipani, Using LDGM codes and sparse syndromes to achieve digital signatures, In: Gaborit, P. (ed.) PQCrypto 2013. LNCS 7932, Springer, Heidelberg (2013) 1-15.

[3] G. Bisson, A. V. Sutherland, Computing the endomorphism ring of an ordinary elliptic curve over a finite field, Journal of Number Theory 131(5) (2011) 815-831.

[4] R. Broker, Constructing supersingular elliptic curves, Journal of Combinatorics and Number Theory 1(3) (2009) 269-273.

[5] D. Boucher, P. Gaborit, W. Geiselmann, O. Ruatta, F. Ulmer, Key exchange and encryption schemes based on non-commutative skew polynomials. In: Sendrier, N. (ed.) PQCrypto 2010. LNCS 6061 (2010) 126-141.

[6] J. Buchmann, E. H. Dahmen, A. ulsing, XMSS - A practical forward secure signature scheme based on minimal security assumptions, In: Yang, B.-Y. (ed.)PQCrypto 2011. LNCS 7071 (2011) 117-129.

[7] P. L. Cayrel, M. Meziani, Post-quantum cryptography: Code-based signatures, In: Kim, T.-H., Adeli, H. (eds.) AST/UCMA/ISA/ACN 2010. LNCS 6059 (2010) 82–99.

[8] C. W. Chan, C. C. Chang, A scheme for threshold multi-secret sharing, Applied Mathematics and Computation 166 (2005) 1-14.

[9] T. Y. Chang, M. S. Hwang, W. P. Yang, A new multi-stage secret sharing scheme using one-way function, ACM SIGOPS Operating Systems 39 (2005) 48-55.

[10] D. X. Charles, E. Kristin, Lauter, Z. G. Eyal, Cryptographic hash functions from expander graphs, Journal of Cryptology 22 (2009) 93-113.

[11] A. Childs, D. Jao, V. Soukharev, Constructing elliptic curve isogenies in quantum sub-exponential time, Journal of Mathematical Cryptology 8(1) (2014) 1– 29.

[12] J. M. Couveignes, Quelques calculs en théorie des nombres, PhD thesis, Université de Bordeaux, 1994.

[13] J. M. Couveignes, Isomorphisms between Artin-Schreier towers, Mathematics of Computation 69(232) (2000) 1625–1631.

[14] J. M. Couveignes, Hard homgeneous spaces, http://eprint.iacr.org/2006/291.

[15] E. Dahmen, K. Okeya, T. Takagi, C. Vuillaume, Digital signatures out of second preimage resistant hash functions. In: Buchmann, J., Ding, J. (eds.) PQCrypto 2008. LNCS 5299 (2008) 109-123.

[16] X. Dong, A Multi-secret sharing scheme based on the CRT and RSA, International Journal of Electronics and Information Engineering 2(1) (2015) 47-51.

[17] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE transactions on information theory 31(4) (1985) 469-472.

[18] N. D. Elkies, Elliptic and modular curves over finite fields and related computational issues, In Computational perspectives on number theory 7 (1995) 21-76.

[19] M. Fatemi, T. Eghlidos, M. Aref, A multi-stage secret sharing scheme using all-or-nothing transform approach, ICICS'09, LNCS 5927 (2009), 449-458.

[20] L. D. Feo, C. Hugounenq, J. Plut, E. Schost, Explicit isogenies in quadratic time in any characteristic, LMS Journal of Computation and Mathematics 19(A) (2016) 267–282.

[21] L. D. Feo, É. Schost, Fast arithmetics in artin-schreier towers over finite fields, In ISSAC '09: Proceedings of the 2009 international symposium on Symbolic and algebraic computation, New York, NY, USA, (2009) 127–134.

[22] L. D. Feo, D. Jao, J. Plut, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, Journal of Mathematical Cryptology 8(3) (2014).

[23] S. D. Galbraith, Constructing isogenies between elliptic curves over finite fields, LMS Journal of Computation and Mathematics 2 (1999) 118–138.

[24] S. D. Galbraith, C. Petit, J. Silva, Signature schemes based on supersingular isogeny problems, To appear in Asiacrypt 2017, Available at eprint 2016/1154.

[25] C. Gentry, C. Peikert, V. Vaikuntanathan, Trapdoors for hard lattices and new cryptographic constructions, In: Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing, (2008) 197-206.

[26] L. Harn, Comment: Multistage Secret Sharing based on One-way Function, Electronics Letters, 31(4) (1995) 62-262.

[27] L. Harn, Effcient Sharing (Broadcasting) of Multiple Secrets, Proceeding of the IEE Comput. Digit. Tech., 142(3) (1995) 237-240.

[28] J. He, E. Dawson, Multisecret-Sharing Scheme Based on One-way Function, Electronic Letters, 31(2) (1995) 93-95.

[29] J. He, E. Dawson, Multi-Stage Secret Sharing Scheme Based on One-way Function, Electronic Letters, 30(19) (1994) 1591-1592.

[30] D. Jao, L. De Feo, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, in Postquantum cryptography, vol. 7071 of Lecture Notes in Comput. Sci. (2011) 19–34.

[31] D. Jao, V. Soukharev, Isogeny-based quantum-resistant undeniable signatures, in Post-Quantum Cryptography, LNCS 8772 (2014) 160-179.

[32] S. Kim, K. Yoon, J. Kwon, S. Hong, Y. H. Park, Efficient Isogeny Computations on Twisted Edwards Curves, Security and Communication Networks Volume 2018, Article ID 5747642, 11 pages

[33] D. R. Kohel, Endomorphism rings of elliptic curves over finite fields [Ph.D. Thesis], University of California, Berkeley, Calif, USA, 1996.

[34] H. X. Li, C. T. Cheng, L. J. Pang, An Improved Multi-Stage (t,n)-Threshold Secret Sharing Scheme, WAIM05, Fan W., Wu Z., and Yang J., eds., LNCS 3739 (2005) 267-274.

[35] R. J. McEliece, A Public-Key Cryptosystem Based On Algebraic Coding Theory, Deep Space Network Progress Report 44 (1978) 114-116.

[36] D. Micciancio, O. Regev, Lattice-based cryptography, In: Bernstein, D.J., Buchmann, J., Dahmen, E. (eds.) Post-Quantum Cryptography (2009) 147-191.

[37] P. L. Montgomery, Speeding the pollard and elliptic curve methods of factorization, Mathematics of Computation 48(177) (1987) 243-264.

[38] N. Patel, P. D. Vyavahare, M. Panchal, A novel verifiable multi-secret sharing scheme based on elliptic eurve cryptography, The tenth international conference on emerging security information, systems and technologies, 2016.

[39] M. S. Srinath, V. Chandrasekaran, Isogeny-based Quantum-resistant Undeniable Blind Signature Scheme, International Journal of Network Security, 20(10) (2018) 9-18.

[40] P. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comput. 26 (1997) 1484-1509.

[41] R. Shi, H. Zhong, L. Huang, A (t, n)-threshold verified multi-secret sharing scheme based on ecdlp, in (IEEE) Eighth ACIS international conference on software engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (2007) 9-13.

[42] J. H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics, 106. Springer, New York (1992) (Corrected reprint of the 1986 original)

[43] J. A. Solinas, Low-weight binary representations for pairs of integers,Technical report, National Security Agency, USA, 2001.

[44] A. 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) (2010) 215–235.

[45] S. Tani, Claw Finding Algorithms Using Quantum Walk, http://arxiv.org/abs/0708.2584, 2008.

[46] J. Tate, Endomorphisms of abelian varieties over finite fields, Invent. Math 2 (1966) 134-144.

[47] E. Teske, The pohlig-hellman method generalized for group structure computation, Journal of Symbolic Computation, 27(6) (1999) 521-534.

[48] J. Velu, Isogenies entre courbes elliptiques, Comptes Rendus Mathematique Academie des Sciences, Paris 273 (1971) 238-241.

[49] L. C. Washington, Elliptic curves, Number theory and cryptography, CRC Press, Boca Raton, 2008.

[50] T. Yasuda, T. Takagi, K. Sakurai, Multivariate signature scheme using quadratic forms, In: Gaborit, P. (ed.) PQCrypto 2013. LNCS, 7932 (2013) 243-258.

[51] Y. Yoo, R. Azarderakhsh, A. Jalali, D. Jao, V. Soukharev, A post-quantum digital signature scheme based on supersingular isogenies, In financial crypto,vol. 2017 (2017).

[52] S. Zhang, Promised and distributed quantum search computing and combinatorics, In proceedings of the eleventh annual international conference on computing and combinatorics, vo 3595 of Lecture notes in computer science, pages 430-439, Berlin, Heidelberg, 2005. Springer Berlin / Heidelberg