ISSN: 1017-060X (Print)

ISSN: 1735-8515 (Online)

Special Issue of the

Bulletin of the

Iranian Mathematical Society

in Honor of Professor Freydoon Shahidi's 70th birthday

Vol. 43 (2017), No. 4, pp. 77–88

Title:

Diffie-Hellman type key exchange protocols based on isogenies

Author(s):

H. Daghigh, R. Khodakaramian Gilan and F. Seifi Shahpar

Published by the Iranian Mathematical Society
http://bims.ims.ir

Bull. Iranian Math. Soc.
Vol. 43 (2017), No. 4, pp. 77–88
Online ISSN: 1735-8515

DIFFIE-HELLMAN TYPE KEY EXCHANGE PROTOCOLS BASED ON ISOGENIES

H. DAGHIGH*, R. KHODAKARAMIAN GILAN AND F. SEIFI SHAHPAR

Abstract. In this paper, we propose some Diffie-Hellman type key exchange protocols using isogenies of elliptic curves. The first method which uses the endomorphism ring of an ordinary elliptic curve E, is a straightforward generalization of elliptic curve Diffie-Hellman key exchange. The method uses commutativity of the endomorphism ring $End(E)$. Then using dual isogenies, we propose a second method. This case uses the endomorphism ring of an elliptic curve E, which can be ordinary or supersingular. We extend this method using isogenies between two elliptic curves E and E'. Our methods have the security level of that of [D. Jao and L. De Feo, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, *J. Math. Cryptol.* 8 (2014), no. 3, 209–247], with the advantage of transmitting less information between two parties.
Keywords: Supersingular elliptic curves, isogeny, cryptography, key exchange.
MSC(2010): Primary: 65F05; Secondary: 46L05, 11Y50.

1. Introduction

A key exchange protocol is the process of securely exchanging a secret key between two or more parties over a public channel. The security of a key exchange protocol is usually based on the hardness of some mathematical problems such as Discrete Logarithm Problem (DLP), the problem of finding positive integer k from a^k in the cyclic group $G = \langle a \rangle$. Diffie-Hellman problem, first proposed by Whitfield Diffie and Martin Hellman in 1976, is the problem of computing a^{kl} from given values of a, a^k and a^l in G. This problem is directly used to construct the Diffie-Hellman key exchange protocol and has become one of the most practical ways for secure key distribution over a public channel.

Different algorithms have been proposed for solving DLP. In particular the index calculus method solves the DLP on the group $\mathbb{F}_q^*$ in subexponential time. Frey and Ruck [5] and Menezes et al. [11] proposed algorithms to reduce

Article electronically published on August 30, 2017.
Received: 4 July 2016, Accepted: 24 March 2017.
*Corresponding author.

the discrete logarithm problem on an elliptic curve E over $\mathbb{F}_q$ to a DLP in some finite field extension $\mathbb{F}_{q^k}$. Menezes et al. [11] also showed that in the supersingular case, one has $k \leq 6$.

On the other hand, many of the mathematical problems which are considered hard, will not remain hard for quantum computers. One of the promising candidates for quantum-resistant cryptography is the isogeny-based cryptography [9]. Stolbunov in [17], proposed a quantum-resistant Diffie-Hellman type system using the class group action on a set of isogenious elliptic curves. The security of this cryptosystem is based on the hardness of the Isogeny Problem (IP), the problem of finding an isogeny between two given isogenious elliptic curves. This method shares a common secret key between two parties by walking on the isogeny graph of ordinary elliptic curves. A few years later, Childs et al. [3] presented an algorithm that could recover these common secret keys in quantum subexponential time.

Later Jao-De Feo [9], proposed a new candidate for quantum-resistant public key cryptosystems based on the difficulty of finding isogeny between supersingular elliptic curves instead of ordinary ones. In this method they construct a commutative diagram which results in the j-invariant of a common curve between two parties.

In this paper, we propose two new Diffie-Hellman type key exchange protocols based on the difficulty of solving isogeny problem along with an extra condition. We recall that the Elliptic Curve Discrete Logarithm Problem (ECDLP) is the problem of finding an integer n such that $Q = nP$, where E is an elliptic curve, $P \in E$ and $Q \in \langle P \rangle$, where by $\langle P \rangle$, we mean the group generated by P. As multiplication-by-n map is an isogeny of the curve E, we can generalize ECDLP to the following problem:

Isogeny Logarithm Problem (ILP): Let E and E' be two isogenous elliptic curves, $P \in E$ and $Q \in E'$. Find an isogeny $\phi : E \to E'$ such that $Q = \phi(P)$, if any.

In this paper, we introduce two new key exchange methods. The first method, which uses the endomorphism ring of an ordinary elliptic curve E, is a straightforward generalization of elliptic curve Diffie-Hellman key exchange. This method uses the commutativity of $End(E)$, the ring of endomorphisms of E, and therefore cannot be applied to supersigular elliptic curves. Our second method, which uses the notion of dual isogenies, works for both ordinary and supersingular elliptic curves. We then generalize this method to a key exchange protocol using isogenies between two elliptic curves E and E'. We also introduce a public key encryption scheme using our key exchange protocol.

The remainder of this paper goes as follows. Section 2 contains a brief summary of some preliminaries on elliptic curves and isogenies. In Sections 3 and 4, we introduce our new key exchange protocols and public key algorithm. Section 5 discusses implementation aspects of the proposed scheme by reviewing

the methods for computing isogenies between elliptic curves and presenting an example. Finally Section 6 is devoted to the security analysis of the proposed algorithms.

2. Preliminaries

In this section we introduce some basic concepts from the theory of elliptic curves and isogenies. For more details see [13, 19].

2.1. Elliptic curves.

Definition 2.1. Let p be a prime number and $q = p^\alpha$, where α is a positive integer. An elliptic curve E over the finite field $\mathbb{F}_q$ is a nonsingular projective plane curve with the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_q$. If $p \neq 2, 3$, one can write the equation in the short form

$$y^2 = x^3 + ax + b,\ a, b \in \mathbb{F}_q.$$

Let E be an elliptic curve defined over the field $\mathbb{F}_q$. The set of $\mathbb{F}_q$-rational points of E is defined as

$$E(\mathbb{F}_q) = \{(x, y) \in E \mid x, y \in \mathbb{F}_q\} \cup \{\mathcal{O}\},$$

where $\mathcal{O}$ is the point at infinity. We also denote $E(\bar{\mathbb{F}}_q)$ simply by E. The set $E(\mathbb{F}_q)$ forms an abelian additive group with $\mathcal{O}$ as the identity element. The n-torsion subgroup of E, denoted by $E[n]$, is the set of points $P \in E(\bar{\mathbb{F}}_q)$ such that $nP = \mathcal{O}$.

For $p \neq 2, 3$, an elliptic curve $E/\mathbb{F}_q$ can be determined (up to isomorphism) by its $j-$invariant defined by

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

2.2. Isogenies.

Definition 2.2. Let E and E' be two elliptic curves defined over a finite field $\mathbb{F}_q$. An isogeny from E to E' is a morphism $\phi : E \to E'$ satisfying $\phi(\mathcal{O}) = (\mathcal{O})$.

For every isogeny $\phi : E \to E'$, the degree of ϕ is the degree of ϕ as an algebraic map and is denoted by $deg(\phi)$. For separable isogeny ϕ, we have $deg(\phi) = |ker(\phi)|$. Two elliptic curves E and E' are l-isogenous if there exists an isogeny of degree l from E to E'. For every l-isogeny $\phi : E \to E'$, there exists an l-isogeny $\widehat{\phi} : E' \to E$ such that $\phi\widehat{\phi} = [l]_{E'}$ and $\widehat{\phi}\phi = [l]_E$, where $[l]_E$ and $[l]_{E'}$ are the multiplication-by-l maps on E and E' respectively. The isogeny $\widehat{\phi}$ is called the dual of ϕ.

By Tate's theorem [18], two elliptic curves are isogenous over a finite field $\mathbb{F}_q$ if and only if they have the same number of points over $\mathbb{F}_q$. The group of isogenies from E to E' is denoted by $Hom(E, E')$ and $End(E) = Hom(E, E)$ is called the endomorphism ring of E. The Frobenius map τ_q is the endomorphism $\tau_q(x, y) = (x^q, y^q)$.

Let E be an elliptic curve defined over $\mathbb{F}_q$. The endomorphism ring of E is either an order in an imaginary quadratic field or an order in a quaternion algebra over $\mathbb{Q}$ (see [13, p. 100]). The curve E is called ordinary in the first case and supersingular in the second case. Equivalently, a curve $E/\mathbb{F}_q$ is ordinary if and only if $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$ and is supersingular if and only if $E[p] = \{0\}$ (see [13, p. 145]).

3. Our key exchange method

We remind that in elliptic curve Diffie-Hellman key exchange protocol, Alice and Bob agree on an elliptic curve E and a point $P \in E$. Then Alice chooses her secret integer a and sends aP to Bob. Similarly Bob chooses his secret integer b and sends bP to Alice. Now Alice and Bob can compute the common key abP. In this section, we present two new methods using the notion of isogenies. First we briefly recall the Jao-De Feo key exchange method [9].

Let $p = \ell_A^{e_A}\ell_B^{e_B} \cdot f \pm 1$ be a prime, where ℓ_A and ℓ_B are two small primes, e_A and e_B are positive integers, and f is some (typically very small) cofactor. Also let E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$ such that $(\ell_A^{e_A}\ell_B^{e_B})^2$ divides $|E(\mathbb{F}_{p^2})|$. Moreover assume that $E[\ell_A^{e_A}] = \langle P_A, Q_A\rangle$ and $E[\ell_B^{e_B}] = \langle P_B, Q_B\rangle$, where $\langle P, Q\rangle$ is the subgroup generated by P and Q. Now Alice and Bob can share a common key as it is described in Figure 1.

FIGURE 1. Jao-De Feo Method.

Parameters:
Prime number $p = \ell_A^{e_A}\ell_B^{e_B} \cdot f \pm 1$, Ellipic curve E, $\{P_A, Q_A\} \subset E[\ell_A^{e_A}]$ and $\{P_B, Q_B\} \subset E[\ell_B^{e_B}]$

Alice		Bob
Chooses two secret numbers $m_A, n_A \in \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$ Compute $\phi_A : E \to E_A$ $E_A = E/\langle [m_A]P_A + [n_A]Q_A\rangle$		Chooses two secret numbers $m_B, n_B \in \mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$ Compute $\phi_B : E \to E_B$ $E_B = E/\langle [m_B]P_B + [n_B]Q_B\rangle$
	$\phi_A(P_B), \phi_A(Q_B), E_A \xrightarrow{\quad}$	
	$\phi_B(P_A), \phi_B(Q_A), E_B \xleftarrow{\quad}$	
Compute $E_{AB} =$ $E_B/\langle [m_A]\phi_B(P_A) + [n_A]\phi_B(Q_A)\rangle$ Compute $j(E_{AB})$		Compute $E_{BA} =$ $E_A/\langle [m_B]\phi_A(P_B) + [n_B]\phi_A(Q_B)\rangle$ Compute $j(E_{BA})$

The common key is $j(E_{AB}) = j(E_{BA})$, since two elliptic curves E_{AB} and E_{BA} are both isomorphic to the curve

$$E/\langle [m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B\rangle.$$

Now we describe our new key exchange protocols. Note that our descriptions in this section are brief. We will see how to choose the parameters and isogenies in Section 5.

Method 1: Alice and Bob agree on an ordinary elliptic curve E over finite field $\mathbb{F}_q$ and a point $P \in E[n]$. Alice chooses an endomorphism $\phi \in End(E)$ and sends $\phi(P)$ to Bob. Similarly Bob chooses $\psi \in End(E)$ and sends $\psi(P)$ to Alice. Then they will have a common key $\phi\psi(P) = \psi\phi(P)$ due to the commutativity of $End(E)$.

FIGURE 2. Method 1.

Parameters: Finite field $\mathbb{F}_q$, Ordinary elliptic curve $E/\mathbb{F}_q$ and $P \in E[n]$		
Alice		Bob
Chooses $\phi_A \in End(E)$		Chooses $\phi_B \in End(E)$
	$\phi_A(P) \longrightarrow$	
	$\phi_B(P) \longleftarrow$	
Computes $\phi_A(\phi_B(P))$		Computes $\phi_B(\phi_A(P))$

The common key is $\phi_A(\phi_B(P)) = \phi_B(\phi_A(P))$.

Note that the above method can not be applied to supersingular elliptic curves, because the points $\phi\psi(P)$ and $\psi\phi(P)$ do not necessarily coincide due to the noncommutativity of $End(E)$. We overcome this obstacle using the properties of dual isogenies.

Method 2: In this method, Alice and Bob agree on an elliptic curve E over $\mathbb{F}_q$ and a point $P \in E[n]$ as public knowledge. Then Alice chooses an endomorphism $\phi_A \in End(E)$ and sends $\phi_A(P)$ to Bob. Similarly, Bob chooses the endomorphism $\phi_B \in End(E)$ and sends $\phi_B(P)$ to Alice.

In the second step, Alice computes $Q = \widehat{\phi}_A(\phi_B(P))$ and $j_1 = j\left(\frac{E}{\langle P, Q\rangle}\right)$. Similarly Bob computes $Q' = \widehat{\phi}_B(\phi_A(P))$ and $j_2 = j\left(\frac{E}{\langle P, Q'\rangle}\right)$. Figure 3, describes Method 2. Proposition 3.1 shows that $j_1 = j_2$ is a common key.

Proposition 3.1. *The values of j_1 and j_2 in the above are equal.*

Proof. Let $\alpha \in End(E)$ and $Tr(\alpha) = \widehat{\alpha} + \alpha = k \in \mathbb{Z}$, then we have

$$\langle P, \widehat{\alpha}(P)\rangle = \langle P, kP - \alpha(P)\rangle = \langle P, \alpha(P)\rangle.$$

Therefore,

FIGURE 3. Method 2.

Parameters: Finite field $\mathbb{F}_q$, Elliptic curve $E/\mathbb{F}_q$, $P \in E[n]$		
Alice		Bob
Chooses $\phi_A \in End(E)$		Chooses $\phi_B \in End(E)$
	$\phi_A(P) \longrightarrow$	
	$\longleftarrow \phi_B(P)$	
Computes $Q = \widehat{\phi}_A(\phi_B(P))$		Computes $Q' = \widehat{\phi}_B(\phi_A(P))$
Output: $j_1 = j(\frac{E}{\langle P,Q\rangle})$		Output: $j_2 = j(\frac{E}{\langle P,Q'\rangle})$

$$j\left(\frac{E}{\langle P, \alpha(P)\rangle}\right) = j\left(\frac{E}{\langle P, \widehat{\alpha}(P)\rangle}\right).$$

Now if we set $\alpha = \widehat{\phi}_B\phi_A$, we have $\widehat{\alpha} = \widehat{\phi}_A\phi_B$. Therefore,

$$\begin{aligned} j_1 &= j\left(\frac{E}{\langle P, Q\rangle}\right) = j\left(\frac{E}{\langle P, \widehat{\phi}_A\phi_B(P)\rangle}\right) \\ &= j\left(\frac{E}{\langle P, \widehat{\phi}_B\phi_A(P)\rangle}\right) = j\left(\frac{E}{\langle P, Q'\rangle}\right) = j_2. \end{aligned}$$

□

In the following generalization of Method 2, we use two isogenous elliptic curves E and E' and isogenies between them, instead of a single elliptic curve E and elements of $End(E)$.

Generalization of Method 2: Alice and Bob agree on two isogenous elliptic curves E and E' and a point $P \in E(\mathbb{F}_q)[n]$. Alice chooses an isogeny $\phi_A : E \to E'$ and sends $\phi_A(P)$ to Bob. Similarly, Bob chooses an isogeny $\phi_B : E \to E'$ and sends $\phi_B(P)$ to Alice.
Now Alice computes $Q = \widehat{\phi}_A(\phi_B(P))$ and $j_1 = j\left(\frac{E}{\langle P, Q\rangle}\right)$. Similarly Bob computes $Q' = \widehat{\phi}_B(\phi_A(P))$ and $j_2 = j\left(\frac{E}{\langle P, Q'\rangle}\right)$. Since for two isogenies $\phi_A, \phi_B \in Hom(E, E')$, the maps $\widehat{\phi}_A\phi_B$ and $\widehat{\phi}_B\phi_A$ are in $End(E)$, as in the proof of Proposition 3.1 we can see that $j_1 = j_2$. This method is summarized in Figure 4.

The advantage of our protocols is that the transmitted information is only $\phi_A(P)$ and $\phi_B(P)$. The exchanged information in [9] includes the image of

FIGURE 4. Generalized Method 2.

Parameters: Finite field $\mathbb{F}_q$, Elliptic curves $E/\mathbb{F}_q$, $E'/\mathbb{F}_q$, and $P \in E[n]$		
Alice		Bob
Chooses $\phi_A \in Hom(E, E')$		Chooses $\phi_B \in Hom(E, E')$
	$\phi_A(P) \longrightarrow$	
	$\phi_B(P) \longleftarrow$	
Computes $Q = \widehat{\phi}_A(\phi_B(P))$		Computes $Q' = \widehat{\phi}_B(\phi_A(P))$
Output: $j_1 = j(\frac{E}{\langle P,Q\rangle})$		Output: $j_2 = j(\frac{E}{\langle P,Q'\rangle})$

the generators of $E[\ell_A^{e_A}]$ and $E[\ell_B^{e_B}]$ under the secret isogenies ϕ_B and ϕ_A respectively.

4. Public key encryption

In this section, we show that our key exchange protocol can be used to construct a public key encryption system, inspired from the way that El-Gamal encryption can be constructed from Diffe-Hellman problem. Let all the notations be the same as before.

Public Parameters: Choose a finite field $\mathbb{F}_q$, two supersingular elliptic curves E and E' over $\mathbb{F}_q$ and a point $P \in E(\mathbb{F}_q)$. Also let $H_k : \mathbb{F}_{p^2} \to \{0,1\}^k$ be a hash function and $k \in \mathbb{Z}$ (see [12, p. 321]).

Key Generation: Choose the isogeny $\phi_{priv} : E \to E'$, a point $P \notin ker(\phi_{priv})$ and compute $Q = \phi_{priv}(P)$. The public key is Q and the private key is the isogeny ϕ_{priv}.

Encryption: For given public key Q and the message $m \in \{0,1\}^k$, choose the isogeny $\phi_{enc} : E \to E'$ and compute

$$\begin{cases} R = \widehat{\phi}_{enc}(Q), \\ S = \phi_{enc}(P), \\ j = j(E/\langle P, R\rangle). \end{cases}$$

Then compute $c = H_k(j) \oplus m$, where $\oplus$ denotes the XOR operation (see [14, p. 550]). The ciphertext is (S, c).

Decryption: Given a ciphertext (S, c), compute

$$\begin{cases} Q' = \widehat{\phi}_{priv}(S), \\ j = j(E/\langle P, Q'\rangle). \end{cases}$$

The plaintext is $m = H_k(j) \oplus c$.

Note that in the above public key encryption, we can use the endomorphisms of a single elliptic curve E instead of isogenies between two curves.

5. **Implementation aspects**

In this section, we discuss the computation of required isogenies and parameters to execute the proposed key exchange protocols. We also give an example.

5.1. **Computing Isogenies.** In order to have an endomorphism on ordinary elliptic curve E over $\mathbb{F}_q$ in Method 1, one can choose two random integers m, n and constructs $m + n\tau_q$, where $q = p^\alpha$ and τ_q is the Frobenius endomorphism. In supersingular cases (Method 2), one can use the following construction. Let $\mathcal{O}$ be a maximal order in the quaternion algebra B_p over $\mathbb{Q}$ ramified at p and ∞ and let $\{1, \alpha_1, \alpha_2, \alpha_3\}$ be the set of generators of $\mathcal{O}$. Using the method of [2], one can construct a supersingular elliptic curve E with endomorphism ring $End(E) = \mathcal{O}$ over $\mathbb{F}_q$. The running time of this method is $O(p^{2.5+\epsilon})$ which can even be reduced to $O(p^{1+\epsilon})$ in some special cases.

For the generalized method, we can select two elliptic curves and an isogeny ϕ between them as follows. Let E be an elliptic curve and G be an arbitrary subgroup of E. Then there exists an elliptic curve E/G (unique up to isomorphism) and an isogeny $\psi : E \to E' = E/G$ with $ker(\psi) = G$. This isogeny can be computed using Velu's formula as follows. Let E be defined by the polynomial $F(x, y) = x^3 + a_2x^2 + a_4x + a_6 - (y^2 + a_1xy + a_3y) = 0$, and S be the set of points of order two in G. Also assume that T is a subset of G such that $G = \{\mathcal{O}\} \cup S \cup T \cup \{-Q \ : \ Q \in T\}$ and $|G| = 1 + |S| + 2|T|$. We compute

$$F_x = \frac{\partial F}{\partial x} = 3x^2 + 2a_2x + a_4 - a_1y \quad and \quad F_y = \frac{\partial F}{\partial y} = -2y - a_1x - a_3.$$

Now for a point $Q = (x_Q, y_Q) \in T \cup S$, define the values
$u(Q) = (F_y(Q))^2$ and

$$t(Q) = \begin{cases} F_x(Q) & \text{if } \ Q \in S, \\ 2F_x(Q) - a_1F_y(Q) & \text{if } \ Q \in T. \end{cases}$$

Set

$$t(G) = \sum_{Q \in T \cup S} t(Q)$$

and

$$w(G) = \sum_{Q \in T \cup S} u(Q) + x_Q t(Q).$$

Then the map $\psi : (x, y) \mapsto (X, Y)$ defined by

$$X = x + \sum_{Q \in T \cup S} \frac{t(Q)}{x - x_Q} + \frac{u(Q)}{(x - x_Q)^2}$$

and

$$Y = y - \sum_{Q \in T \cup S} u(Q)\frac{2y + a_1x + a_3}{(x - x_Q)^3} + t(Q)\frac{a_1(x - x_Q) + y - y_Q}{(x - x_Q)^2} + \frac{a_1u(Q) - F_x(Q)F_y(Q)}{(x - x_Q)^2}$$

is a separable isogeny from E to

$$E' : Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6,$$

where $A_1 = a_1,\ A_2 = a_2, A_3 = a_3, A_4 = a_4 - 5t(G)$, and $A_6 = a_6 - (a_1^2 + 4a_2)t(G) - 7w(G)$. The kernel of this isogeny is the subgroup G and the running time for this algorithm is $O(|G|)$ (see [7, p. 517]).

In the case where $G = \langle R\rangle$ is cyclic with order $|G| = \ell^e$, Jao-De Feo [9] presented a more efficient method to compute the isogeny ψ. In their method ψ decomposes as a chain of ℓ-isogenies. Set $E_0 = E$, $R_0 = R$, and for $0 \le i < e$,

$$E_{i+1} = E_i/\langle \ell^{e-i-1}R_i\rangle, \qquad \psi_i : E_i \to E_{i+1}, \qquad R_{i+1} = \psi_i(R_i).$$

Then we construct the isogeny $\psi : E \longrightarrow E'$ with $E = E_0$, $E' = E_e = E/\langle R\rangle$ and $\psi = \psi_{e-1}\cdots\psi_0$. In each step, the curve E_{i+1} and the isogeny ψ_i can be computed by Velu's formula.

Finally using the generated isogeny ψ and the generators $\{1, \alpha_1, \alpha_2, \alpha_3\}$ of $\mathcal{O}$, we make public the four isogenies $\phi_0 = \psi$, $\phi_1 = \psi \circ \alpha_1$, $\phi_2 = \psi \circ \alpha_2$ and $\phi_3 = \psi \circ \alpha_3$ from E to E'.

Now in the generalized method, Alice chooses random integers a_0, a_1, a_2, a_3 and sets $\phi_A = a_0\phi_0 + a_1\phi_1 + a_2\phi_2 + a_3\phi_3$. Similarly Bob chooses b_0, b_1, b_2, b_3 and sets $\phi_B = b_0\phi_0 + b_1\phi_1 + b_2\phi_2 + b_3\phi_3$. Moreover, for the ℓ-isogeny $\phi : E \to E'$, since $ker(\widehat{\phi}) = \phi(E[\ell])$, one can compute the dual isogeny $\widehat{\phi}$ using the above procedure.

5.2. **Example.** We present an example in the following two steps. We have used the SAGE software [15, 16] for our computations. In every key exchange process, Alice can construct isogeny ϕ_A using a linear combination of the isogenies ϕ_0, ϕ_1, ϕ_2, and ϕ_3 to execute the protocol.

Setup: Let $\mathbb{F}_{503^2} = \mathbb{F}_{503}(w)$, where $w^2 + w + 1 = 0$. Also let $E : y^2 = x^3 - 1$ and $G = (496, 320w + 160) \in E$. We also choose a point $P = (258w + 158, 210w + 90) \in E[504]$. Using Velu's formula, we compute

$$\psi : E \to E/\langle G\rangle = E',$$

where $E' : y^2 = x^3 + 159x + 155$.

The endomorphism ring of E is an order in the quaternion algebra $B_{503} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$, where $i^2 = -3$, $j^2 = -503$ and $ij = k = -ji$. Here

$$i : (x, y) \longmapsto (X, Y),$$

where

$$X = -\frac{9}{4}\,wx^7 + 2\,wx - x + \frac{\left(\frac{9\left(wx^4 - 4\,wx\right)w^2x^2y}{x^3-1} - 16\,y\right)^2}{4\left(9\,wx^7 - 8\,wx - 4\,x - 16\right)^2} + 4,$$

and

$$Y = -\frac{9\left(wx^4 - 4\,wx\right)w^2x^2y}{8\,(x^3-1)} + y.$$

We also have

$$j : (x, y) \longmapsto (wx, y).$$

In fact $End(E)$ is the order $End(E) = \mathbb{Z} + \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \mathbb{Z}\alpha_3$ in B_{503}, where

$$\alpha_1 = 1/2(-1+i),\ \alpha_2 = j,\ \alpha_3 = 1/6(3+i+3j+k).$$

We have

$$\begin{aligned} \alpha_1 : (x, y) &\longrightarrow (wx, y), \\ \alpha_2 : (x, y) &\longrightarrow (x^{503^2}, (x^3-1)^{126504}y). \end{aligned}$$

Set $\phi_0 = \psi$, $\phi_1 = \psi \circ \alpha_1$, $\phi_2 = \psi \circ \alpha_2$ and $\phi_3 = \psi \circ \alpha_3$.

Key Exchange: Alice chooses $\phi_A = \phi_0 + 2\phi_1$ and sends $\phi_A(P) = (163w + 197, 81w + 224)$ to Bob. Similarly Bob chooses $\phi_B = 3\phi_0 + \phi_1 + 2\phi_2$ and sends $\phi_B(P) = (359w + 317, 88w + 356)$ to Alice.
Now Alice computes

$$Q = \widehat{\phi}_A(\phi_B(P)) = (304w + 318, 154w + 273)$$

and $E/\langle P, Q\rangle : y^2 = x^3 + (333w + 135)x + 278w + 385$ and obtains

$$j_1 = j(E/\langle P, Q\rangle) = 1728(\frac{4(333w+135)^3}{4(333w+135)^3 + 27(278w+385)^2}) = 283w + 459.$$

Similarly Bob computes

$$Q' = \widehat{\phi}_B(\phi_A(P)) = (318w + 304, 349w + 119)$$

and $E/\langle P, Q'\rangle : y^2 = x^3 + (333w + 135)x + 278w + 385$ and obtains

$$j_2 = j(E/\langle P, Q'\rangle) = 1728(\frac{4(333w+135)^3}{4(333w+135)^3 + 27(278w+385)^2}) = 283w + 459.$$

Therefore the common key is $283w + 459$.

6. **Security analysis**

In this section, we analyse the security of the proposed algorithms, as well as listing some problems that their hardness is the basis of the security of our protocols.

As before, let E and E' be two supersingular elliptic curves, ϕ_A and ϕ_B be two isogenies from E to E', and $P \in E[n]$. In the following, we define some problems which are very important from security point of view and solving any one of them leads to breaking our protocols.

Problem 1 (Isogeny Problem (IP)): For two given isogenious elliptic curves E and E', find an isogeny $\phi : E \to E'$.

Problem 2 (Isogeny Logarithm Problem (ILP)): Let E and E' be two isogenous elliptic curves, $P \in E$ and $Q \in E'$. Find an isogeny $\phi : E \to E'$ such that $Q = \phi(P)$, if any.

Problem 3 (Computational Isogeny-based Diffie-Hellman Problem (CIDH)): For two isogenies $\phi_A, \phi_B : E \to E'$ and the point $P \in E[n]$, let E' and the points $Q_1 = \phi_A(P)$ and $Q_2 = \phi_B(P)$ be given. Compute $j\left(\frac{E}{\langle P, \widehat{\phi}_A(\phi_B(P))\rangle}\right)$ or $j\left(\frac{E}{\langle P, \widehat{\phi}_B(\phi_A(P))\rangle}\right)$ from Q_1 and Q_2.

Problem 1 is a hard problem that has been studied by many authors [3, 10, 6, 8, 17]. In 2013, Galbraith and Stolbunov [8] introduced an algorithm which solves the isogeny problem over finite field $\mathbb{F}_q$ in $\tilde{O}(q^{1/4})$, where $\tilde{O}$ denotes the complexity with the logarithmic factors omitted. In the case of supersingular elliptic curves, one can use Delfs and Galbraith classical algorithm which solves the isogeny problem in $\tilde{O}(p^{1/2})$ operations, where p is the characteristic of the base field [4]. Also the quantum algorithm proposed by Biass et al. [1] solves the isogeny problem with complexity $\tilde{O}(p^{1/4})$.

Problem 2 is even harder, because it must satisfy the extra condition $Q = \phi(P)$. In general, there is no effective algorithm to find an isogeny between two elliptic curves as mentioned before and it seems hard to determine the structure of $Hom(E, E')$. Note that in supersingular elliptic curve E, the endomorphism ring of E has rank four, while $E[n]$ is generated by two elements. So for the basis $\{1, \alpha_1, \alpha_2, \alpha_3\}$ of $End(E)$, the coefficients of the equation $\phi(P) = mP + n\alpha_1(P) + r\alpha_2(P) + s\alpha_3(P)$ can not be uniquely determined. Therefore, finding the isogeny $\phi = m + n\alpha_1 + r\alpha_2 + s\alpha_3$ from $\phi(P) = mP + n\alpha_1(P) + r\alpha_2(P) + s\alpha_3(P)$ seems to be hard.

In Problem 3, since the isogeny problem has not yet been solved, it is reasonable to assume that the question of computational isogeny-based Diffie-Hellman problem is hard to solve.

Acknowledgements

We would like to thank the referees for their careful reading and valuable comments. This research is partially supported by the University of Kashan under grant number 159037/1.

References

[1] J.F. Biasse, D. Jao and A. Sankar, A quantum algorithm for computing isogenies between supersingular elliptic curves, in: Progress in Cryptology–INDOCRYPT 2014, pp. 428–442, Lecture Notes in Comput. Sci. 8885, Springer, Cham, 2014.

[2] I. Chevyrev and S.D. Galbraith, Constructing supersingular elliptic curves with a given endomorphism ring, *LMS J. Comput. Math.* **17** (2014), no. 2, 71–91.

[3] A. Childs, D. Jao and V. Soukharev, Constructing elliptic curve isogenies in quantum subexponential time, *J. Math. Cryptol.* **8** (2014), no. 1, 1–29.
[4] C. Delfs and S.D. Galbraith, Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$, *Des. Codes Cryptogr.* **78** (1999), no. 2, 425–440.
[5] G. Frey and H.G. Ruck, A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves, *Math. Comp.* **62** (1994), no. 206, 865–874.
[6] S.D. Galbraith, Constructing isogenies between elliptic curves over finite fields, *LMS J. Comput. Math.* **2** (1999) 118–138.
[7] S.D. Galbraith, Mathematics of Public Key Cryptography, Cambridge Univ. Press, 2012.
[8] S.D. Galbraith and A. Stolbunov, Improved algorithm for the isogeny problem for ordinary elliptic curves, *Appl. Algebra Engrg. Comm. Comput.* **24** (2013), no. 2, 107–131.
[9] D. Jao and L. De Feo, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, *J. Math. Cryptol.* **8** (2014), no. 3, 209–247.
[10] D. Kohel, Endomorphism rings of elliptic curves over finite fields, PhD Thesis, University of California at Berkeley, 1996.
[11] A.J. Menezes, T. Okamoto and S.A. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, *IEEE Trans. Inform. Theory* **39** (1993), no. 5, 1639–1646.
[12] A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.
[13] J.H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, 2nd edition, New York, 2009.
[14] R.E. Simpson, Introductory Electronics for Scientists and Engineers, Addison-Wesley, 2nd edition, 1987.
[15] W.A. Stein and D. Joyner, SAGE: system for algebra and geometry experimentation, *Commun. Comput. Algebra* **39** (2005) 61–64.
[16] W.A. Stein, SAGE: software for algebra and geometry experimentation, http://www.sagemath.org.
[17] A. Stolbunov, Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves, *Adv. Math. Commun.* **4** (2010), no. 2, 215–235.
[18] J. Tate, Endomorphisms of abelian varieties over finite fields, *Invent. Math* **2** (1966) 134–144.
[19] L.C. Washington, Elliptic Curves, Number Theory and Cryptography, CRC press, 2nd edition, 2008.

(Hassan Daghigh)
E-mail address: hassan@kashanu.ac.ir

(Ruhulla Khodakaramian Gilan)
E-mail address: rkhodakaramian@grad.kashanu.ac.ir

(Fatemeh Seifi Shahpar)
E-mail address: fatemeh.seifishahpar@gmail.com