Journal of Information Hiding and Multimedia Signal Processing ©2014 ISSN 2073-4212
Ubiquitous International Volume **5**, Number **4**, October **2014**

Elliptic Curve Isogenies-Based Three-party Password Authenticated Key Agreement Scheme towards Quantum-Resistant

Hongfeng Zhu, Xin Hao, and Yang Sun

Software College, Shenyang Normal University
No.253, HuangHe Bei Street, HuangGu District, Shenyang, P.C 110034 - China
{zhuhongfeng1978@163.com, {839940028, 17247613}@qq.com}

Received February, 2014; revised April, 2014

Abstract. *Since quantum computers came on the scene, the world has changed greatly, especially related to cryptography. Public key cryptosystem, particularly RSA cryptosystem cant resist the quantum computers attack, so some quantum-resistant schemes have been proposed mainly based on quantum key distribution (QKD) method or new resistance to quantum algorithms. However, to the best of our knowledge, no elliptic curve isogenies-based practical three-party password-authenticated key agreement (3PAKA) protocol without using a timestamp has been proposed, yet. In this paper, we propose the first elliptic curve isogenies-based 3PAKA protocol without a timestamp towards quantum-resistant. We give a full specification of the proposed scheme, including how to realize specific properties by analyzing cryptography tools, how to design the scheme, how to prove the scheme's security based on the three isogeneous problems on elliptic curves. Up to now, about quantum-resistant of the scheme, the fastest known attacks against our scheme, even on quantum computers, require fully exponential time.*
Keywords: Security Protocol; Key Exchange; Elliptic Curve Isogenies; Quantum-Resistant.

1. **Introduction.** Advances in quantum computers pose great threats on the currently used public key cryptographic algorithms such as RSA and ECC [1, 2, 41, 42]. So people hope to find having properties of public-key cryptography just like quantum cryptographic protocol [3], and we called them Quantum Public-key Cryptography (QPKC). The related research can mainly be divided into two kinds:

(1) Quantum physics-based methodology. Quantum cryptography, which began with Wiesner's idea [55] almost 40 years ago, has reached the stage of commercial key distribution devices [56–58]. Origin of quantum key distribution in its oldest form is belonged to Bennett and Brassard [59] in 1984. This pioneering work was named as BB84 protocol. Next, Bennett [60] again proposed another quantum cryptographic protocol using any two non-orthogonal states where the two parties share no secret initially. Generalization of BB84 quantum cryptographic protocol using three conjugate bases [61], quantum key distribution in the holevo limit [62] and extension of BB84 protocol in terms of encoding in N-dimensional Hilbert space [63] are some of the developments in the context of quantum key distribution. Furthermore, many research areas can be summarized as below: (a) Quantum secret sharing protocols [64]. (b) Based on the quantum mechanics which can chase the Public-key Cryptography of perfect security [4, 5]. (c) Without establishing

any shared secret key to achieve secure direct communication [65]. (d) Using multipartite entanglement to design kinds of secure protocols [66].

To sum up, the security of this kind method can be guaranteed by principle of quantum physics which can achieve perfect secrecy if not considering social engineering attacks and some flaws about designing protocol, but it's hard to control the quantum key, lack of flexibility, narrow application recently and so on.

(2) Computational complexity-based methodology. This kind method aims to find hard problems under the quantum computation and according to these hard problems to structure the Public-key Cryptography and security protocol [6-9]. These schemes are very flexible which can be imagined a bridge between electronic computer and quantum computer. Furthermore, many research areas based on computational complexity can be summarized as below: (a) Multivariate Quadratic Polynomials Public Key Cryptosystems [67, 68]. (b) Merkle put forward the signature based on authenticated tree in 1989 [69]. (c) Error correction coding public key cryptosystem [70]. (d) NTRU (Number Theory Research Unit) public key cryptosystem [71]. The article is belonging to the second kind.

The chief aim of this paper is to design a practical security protocol towards quantum-resistant for convenience of customers. On the one hand, we choose the components [23, 43-45] of quantum-resistant to design our protocol. On the other hand, password-based, ID-based and other user-friendly protocols are all good angles to cut into. Until now a lot of user-friendly authenticated key agreement schemes have been proposed [10-21, 73, 74] which are all mainly focus on two or more secure properties and different secure algorithms. For example, the literatures [10-15] mainly adopt chaotic maps as the secure algorithms and different secure properties for different literatures, such as biometric-based, user anonymity, using smart cards and so on. The literature [16] focuses on Identity-based and multiple keys to produce. The literatures [18, 19] research the group key agreement with password-based. And the literatures [73, 74] mainly care about key exchange protocol under the mobile environments.

However, all above-mentioned user-friendly authenticated key agreement schemes can't resist quantum computers attack. To the best of our knowledge, no three-party authenticated key agreement protocol based on elliptic curve isogenies has been proposed, yet. Generally speaking, a 3PAKA protocol with elliptic curve isogenies should achieve the following requirements:

(1) It should allow two users establish a secure session key over an insecure communication channel with the help of a trusted server with the shared passwords.

(2) The trusted server should not get any sensitive information about the session key shared between the two users. The trusted server can only help two users to authenticate each other and transfer the information about how to compute session key.

(3) The protocol should be based on elliptic curve isogenies that can resist quantum attack on algorithm level.

(4) The protocol should be able to resist all known attacks on protocol level, such as password guessing attacks, impersonation attacks, man-in-the-middle attacks, etc.

(5) The protocol should achieve some well-known properties, such as perfect forward secrecy, no timestamp, and execution efficiency.

In this paper, based on elliptic curve isogenies, we propose a new three-party password-authenticated key agreement protocol which achieves the above requirements. The rest of the paper is organized as follows: We outline preliminaries in Section 2. Next, an elliptic curve isogenies-based three-party password authenticated key agreement protocol is described in Section 3. Then, the security analysis and efficiency analysis are given in Section 4 and Section 5. This paper is finally concluded in Section 6.

2. Preliminaries.

2.1. Isogenies.

Definition 1 An isogeny φ [46] is a nontrivial (non-constant) rational map (such as: $\varphi(x,y) = (\frac{f_1(x,y)}{g_1(x,y)}, \frac{f_2(x,y)}{g_2(x,y)})$ of an Elliptic Curve onto another Elliptic Curve that is also a group homomorphism (satisfying $\varphi(\infty) = \infty$,equivalently $\varphi(P+Q) = \varphi(P) + \varphi(Q)$).

Lemma 1 The degree of an isogeny is its degree as an algebraic map [46].

Lemma 2 The endomorphism ring End(E) is the set of isogenies from E($\overline{F}$)to itself, together with the constant homomorphism. This set forms a ring under pointwise addition and composition [46].

Lemma 3 If $\varphi : E \to E'$ is an isogeny, then φ is surjective. Meaning that for a point *P in E ($\overline{K}$) there exists a point P in E($\overline{K}$)such that φ(P) is P [47].*

Definition 2 *Let $\varphi : E \to E'$ be an isogeny, and let $r_1(x)$ be the x-coordinate map. If the derivative of the x-coordinate map $r_1'(x)$ is not 0 then φ is separable [48].*

Definition 3 *An elliptic curve is called supersingular if $E[p] = \{\infty\}$, where $p = char.(E)$ [49].*

Proposition 1 *$E / F_q, q = p^r$. Let $a = q + 1 - \#E(F_q)$ $\to$ E is supersingular if and only if $a \equiv 0 (\mathrm{mod}\ p) \Leftrightarrow E(F_q) \equiv 1 (\mathrm{mod}\ p)$ [49].*

Theorem 3 *For every finite subgroup $G \subset E(\overline{F})$, there exists a unique (up to isomorphism) elliptic curve E / G and a unique (up to isomorphism) separable isogeny $E \to E / G$ of degree $\#G$. (Remark: Every separable isogeny arises in this way[49].)*

Corollary 1 *Every separable isogeny φ factors into a composition of prime degree isogenies[49].*

Theroem 4 *Two curves E and E' are isogenous over $\mathbb{F}_q$ if and only if $\#E = \#E'$. (Remark: The cardinality $\#E$ of E can be calculated in polynomial time using Schoof's algorithm, which is also based on isogenies[50].)*

2.2. Velu Approach: Computing from points in the kernel.

$Ve'lu's$ formulas[22] show how, for any field K, given a Curve E_1/K and the Kernel of an isogeny (as a list of the points of a finite order subgroup of $E(\overline{K})$ how to determine the codomain of the isogeny, as well as compute the isogeny.

Input: Given a cruve in general Weierstrass form:

$E_1 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, and a set of points of C that forms a finite subgroup of $E_1(\overline{K})$.

Output: The general Weierstrass coefficients of a Weierstrass model for the codomain curve E2 of a separable normalized isogeny with kernel C. Also, coordinate maps (as rational maps on E1) that evaluate a point (x, y) on E1 to a point on E2.

Step 1*: Partition the set of points C:*

(1) Throw out ∞.

(2) Let C2 be all the 2-torsion points in C; let R be the rest of the points in C.

(3) Split R into two equal sized sets such that R_+ and R_- so that if a point P is in R_+ then -P is in R_-.

(4) Let $S = R_+ \bigcup C_2$.

Step 2*: Now given $Q \in S$ define the following quantities:*

$g_Q^x = 3x_Q^2 + 2a_2x_Q + a_4 - a_1y_Q, \quad g_Q^y = -2y_Q - a_1x_Q - a_3$

$v_Q = g_Q^x$, if $2Q = \infty$, $v_Q = 2g_Q^x - a_1g_Q^y$,

otherwise $u_Q = (g_Q^y)^2$; $v = \sum_{Q \in S} v_Q$, $w = \sum_{Q \in S} (u_Q + x_Q v_Q)$

Step 3*: Compute the target image: First define the values:*

$A_1 = a_1, A_2 = a_2, A_3 = a_3, A_4 = a_4 - 5v, A_6 = a_6 - (a_1^2 + 4a_2)v - 7w$.

Then the Weierstrass equation of E2 is:

$y^2 + A_1xy + A_3y = x^3 + A_2x^2 + A_4x + A_6$.

Step 4*: The formula for computing the image point (* α, β *)form the point (x, y):*

$$\alpha = x + \sum_{Q \in S} \left(\frac{v_Q}{x - x_Q} - \frac{u_Q}{(x - x_Q)^2}\right),$$

$$\beta = y - \sum_{Q \in S} \left(u_Q \frac{2y + a_1x + a_3}{(x - x_Q)^3} + v_Q \frac{a_1(x - x_Q) + y - y_Q}{(x - x_Q)^2} + \frac{a_1u_Q - g_Q^x g_Q^y}{(x - x_Q)^2}\right)$$

Note that while Velu's formulas clearly can be used to evaluate an isogeny (given the domain and kernel) at a given point of the domain curve, here we are treating Velu's formulas as a way to precompute the rational maps of the isogeny. These rational maps can be stored and used to evaluate any number of points on the domain curve.

2.3. **One-way Hash Function.** *A secure cryptographic one-way hash function* $h: a \to b$ *has four main properties:*

(1) The function h *takes a message of arbitrary length as the input and produces a message digest of fixed-length as the output;*

(2) The function h *is one-way in the sense that given* a*, it is easy to compute* $h(a) = b$*. However, given* b*, it is hard to compute* $h^{-1}(b) = a$*;*

(3) Given a*, it is computationally infeasible to find* a' *such that* $a' \neq a$*, but* $h(a') = h(a)$*;*

(4) It is computationally infeasible to find any pair a*,* a' *such that* $a' \neq a$*, but* $h(a') = h(a)$*.*

2.4. **One-way Hash Function.** *A symmetric encryption scheme* $E_k(Kgen, E, D)$ *consists of three algorithms as follows:*

(1) Randomized Key Generation Algorithm $Kgen$*: it returns a key k drawn from the key space* $Keys(E_k)$ *at random.*

(2) Encryption Algorithm E*: it takes the key* $k \in Keys(E_k)$ *and a plaintext* $M \in \{0,1\}^*$ *as the inputs and outputs a ciphertext* $C \in \{0,1\}^*$*. We write* $C = E_k(M)$*.*

(3) Decryption Algorithm D*: it takes the key* $k \in Keys(E_k)$ *and a ciphertext* $C \in \{0,1\}^*$ *as the inputs and outputs a plaintext* $M \in \{0,1\}^*$*. We write* $M = E_k(C)$*.*

3. The proposed scheme.

3.1. Setting parameters and basic block.

3.2. The proposed scheme.

In this section, we propose a elliptic curve isogenies-based three-party password authenticated key agreement scheme which consists of two phases: the setup phase and the authentication and key agreement phase

Setup phase In this phase, a server S chooses its public key $(E_0, (P_S, Q_S))$ and a pair of secret key (m_S, n_S) based on elliptic curve isogenies, a secure one-way hash function H

Table 1. Notations

Symbol	***Definition***
ID_A, ID_B, ID_S	*Identity information of the Alice, Bob and Server*
$E_K()/D_K()$	*A pair of secure symmetric encryption/decryption functions with the key K which can can resist quantum attack*
$\|\|$	*Means that two adjacent messages are concatenated*
H	*A secure one-way hash function can resist quantum attack*
SK	*Session Key*
$E_0, (P_s, Q_s)$	*Public key of the Server S*
(m_s, n_s)	*Secret key of the Server S*
$(m_A, n_A), (m'_A, n'_A)$ $(m_B, n_B), (m'_B, n'_B)$	*Temporary number of Alice and Bob chosen based on the bases*
$(P_A, Q_A), P'_A, Q'_A)$ $(P_B, Q_B), P'_B, Q'_B)$	*Bases of Alice and Bob based on*
K	*A field*
$\overline{K}$	*A fixed algebraic closure of K*
E	*A fixed elliptic curve given by the Weierstrass model with coecients in K*
$E(K), E(\overline{K})$	*The set of pairs (x, y) satisfying the Weierstrass equation of E where x and y are taken in K or $\overline{K}$ respectively*
φ	*An isogeny from E to another elliptic curve E'*
pw_A	*Shared by Alice and Server*
pw_S	*Shared by Bob and Server*
l_A, l_B, l_S	*Small primes*
f_1, f_2, f_3	*Cofactors*
e_A, e_B, e_S, e_A, e_S	*Positive integer*

against quantum attack, secure symmetric encryption/decryption functions $E_K()/D_K()$ with key K. Additionally, the server S shares passwords pw_A and pw_A with users Alice and Bob; users Alice and Bob choose their identities ID_A andID_B respectively.

Authentication and key agreement phase

In this phase, users Alice and Bob can authenticate each other and establish a session key with the help of the trusted server S. **Figure 1** illustrates this phase.

Round 1 Based on the public information $E_0, (P_S, Q_S) = E_0[l_S^{e_S}]$, Alice chooses bases $(P_A, Q_A) = E_0[l_A^{e_A}]$ and $(m_A, n_A) \in_R Z/l_A^{e_A}Z$. We can fix $F_q = F_{p^2}$ as the field of definition specially, where p is a prime of the form $l_A^{e_A} l_S^{e_S}.f_1 \pm 1$. Here l_A,l_S are small primes, and f_1 is a cofactor such that p is prime, and e_A, e_S are positive integers. Then Alice computes ϕ_{AS}:$E_0/\langle [m_A]\, P_A + [n_A]\, Q_A\rangle$,$E_{AS} : \phi_{AS}(P_S), \phi_{AS}(Q_S)$, where $\ker(\phi_{AS}) = \langle [m_A]\, P_A + [n_A]\, Q_A\rangle$. Finally Alice sends messages $\{(P_A, Q_A), ID_A, E_{AS}, \phi_{AS}(P_S), \phi_{AS}(Q_S)\}$ to S. Similarly , Bob chooses bases $(P_B, Q_B) = E_0[l_B^{e_B}]$ and$(m_B, n_B) \in_R Z/l_B^{e_B}Z$. We can fix $F_q = F_{p^2}$ as the field of definition specically, where p is a prime of the form $l_B^{e_B} l_S^{e_S}.f_2 \pm 1$. Here l_B,l_S are small primes, and f_2 is a cofactor such that p is prime , and e_B, e_S are positive integers. Then Bob computes ϕ_{BS}:$E_0/\langle [m_B]\, P_B + [n_B]\, Q_B\rangle$and $E_{BS} : \phi_{BS}(P_S), \phi_{BS}(Q_S)$, where $\ker(\phi_{BS}) = \langle [m_B]\, P_B + [n_B]\, Q_B\rangle$. Finally Bob sends message to server S.

Round 2 Upon receiving $\{(P_A, Q_A), ID_A, E_{AS}, \phi_{AS}(P_S), \phi_{AS}(Q_S)\}$, $\{(P_B, Q_B), ID_B, E_{BS}, \phi_{BS}(P_S), \phi_{BS}(Q_S)\}$ from Alice and Bob, server S firstly computes ϕ_S:$E_0/\langle [m_S]\, P_S + [n_S]\, Q_S\rangle$, $E_{SA} : \phi_S(P_A), \phi_S(Q_A)$ and $E_{SB} : \phi_S(P_B), \phi_S(Q_B)$, where

$\ker(\phi_S) = \langle [m_S]P_S + [n_S]Q_S \rangle$. Secondly S can compute the $K_{SA} = j(E_{SA-AS})$ and $K_{SB} = j(E_{SB-BS})$ for preparation to use. Then S selects bases $(P'_A, Q'_A) = E_0[(l'_A)^{e'_A}$ and $(P'_B, Q'_B) = E_0[(l'_B)^{e'_B}$, and fixs $F_q = F_{p^2}$ as the field of definition specically, where p is a prime of the form $(l'_A)^{e'_A}(l'_B)^{e'_B}.f_3 \pm 1$. Here l'_A,l'_B are small primes, and f_3 is a cofactor such that p is prime, and e'_A, e'_B are positive integers. Finally S sends messages $(P'_A, Q'_A), (P'_B, Q'_B), ID_S, E_{SA}, \phi_S(P_A), \phi_S(Q_A)$ and $(P'_A, Q'_A), (P'_B, Q'_B), ID_S, E_{SB}, \phi_S(P_B), \phi_S(Q_B)$ to Alice and Bob respectively.

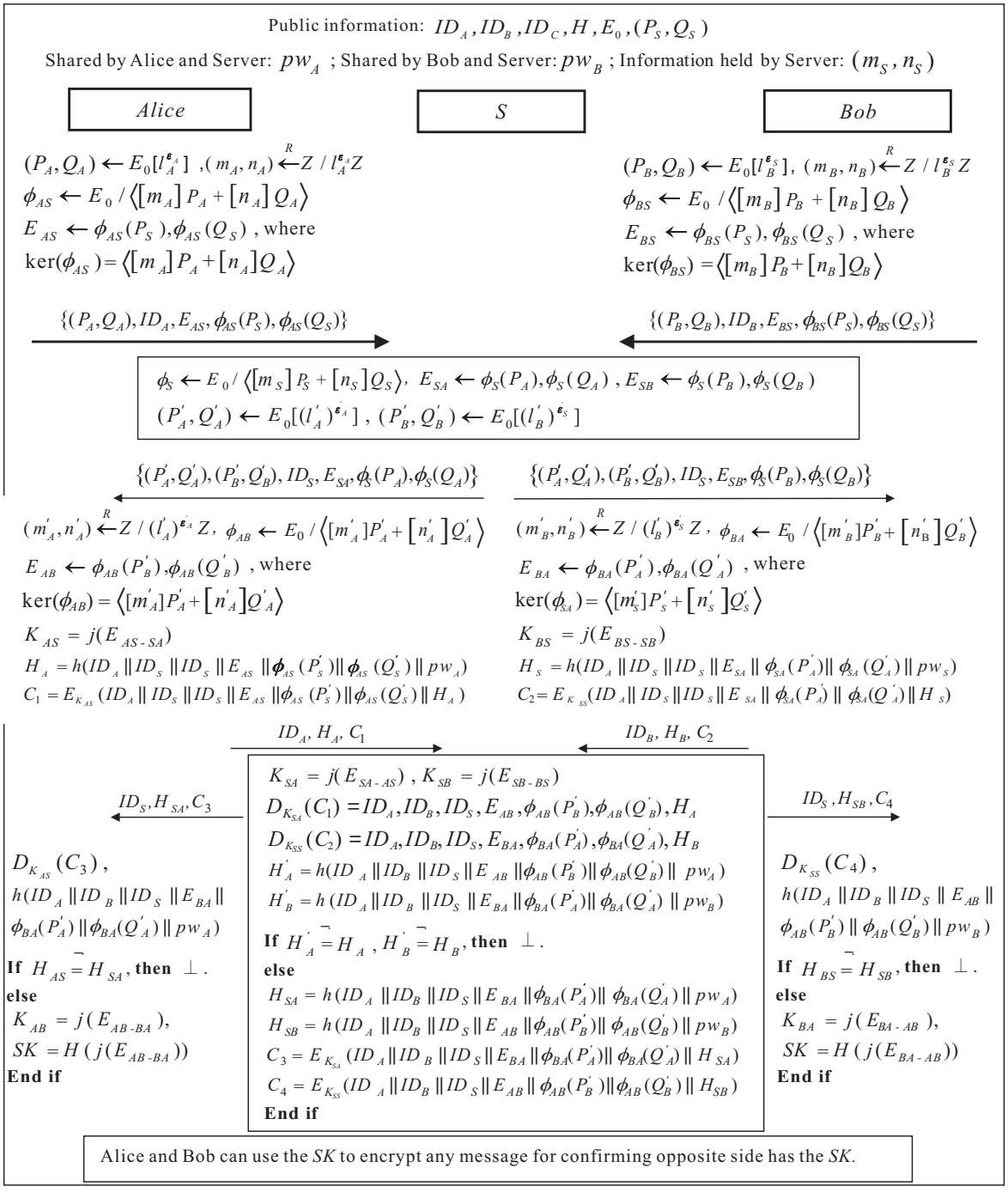

FIGURE 1. Authentication and key agreement phase

Round 3 After receiving the messages $(P_A^{'}, Q_A^{'}), (P_B^{'}, Q_B^{'}), ID_S, E_{SA}, \phi_S(P_A), \phi_S(Q_A)$, Alice firstly computes the session key $K_{AS} = j(E_{AS-SA})$ between Alice and server S based on $E_{SA}, \phi_S(P_A), \phi_S(Q_A)$. Then Alice chooses $(m_A^{'}, n_A^{'}) \in_R Z/(l_A^{'})^{e_A^{'}}Z$ and computes ϕ_{AB}: $E_0/\langle [m_A^{'}]P_A^{'} + [n_A^{'}]\, Q_A^{'}\rangle$,$E_{AB}$: $\phi_{AB}(P_B^{'}), \phi_{AB}(Q_B^{'})$, where $\ker(\phi_{AB}) = \langle [m_A^{'}]P_A^{'} + [n_A^{'}]\, Q_A^{'}\rangle$.

Finally Alice computes $H_A = h(ID_A||ID_B||ID_S||E_{AB}||\phi_{AB}(P_B^{'})||\phi_{AB}(Q_B^{'})||pw_A)$ and $C_1 = E_{K_{AS}}(ID_A||ID_B||ID_S||E_{AB}||\phi_{AB}(P_B^{'})||\phi_{AB}(Q_B^{'})||H_A)$ and sends ID_A, H_A, C_1 to the server S. For Bob, just doing the same things as Alice.

Round 4 After receiving the messages ID_A, H_A, C_1 and ID_B, H_B, C_2, server S can decrypt C_1 and C_2 based on $K_{SA} = j(E_{SA-AS})$ and $K_{SB} = j(E_{SB-BS})$. S continues to compute the $H_A^{'} = h(ID_A||ID_B||ID_S||E_{AB}||\phi_{AB}(P_B^{'})||\phi_{AB}(Q_B^{'})||pw_A)$ using shared pw_A and $H_B^{'} = h(ID_A||ID_B||ID_S||E_{BA}||\phi_{BA}(P_A^{'})||\phi_{BA}(Q_A^{'})||pw_B)$ with pw_B. S check if $H_A^{'} = H_A$ and $H_B^{'} = H_B$.

If holds, S then computes

$H_{SA} = h(ID_A||ID_B||ID_S||E_{BA}||\phi_{BA}(P_A^{'})||\phi_{BA}(Q_A^{'})||pw_A)$

$H_{SB} = h(ID_A||ID_B||ID_S||E_{AB}||\phi_{AB}(P_B^{'})||\phi_{AB}(Q_B^{'})||pw_B)$

$C_3 = E_{K_{SA}}(ID_A||ID_B||ID_S||E_{BA}||\phi_{BA}(P_A^{'})||\phi_{BA}(Q_A^{'})||H_{SA})$

$C_4 = E_{K_{SB}}(ID_A||ID_B||ID_S||E_{AB}||\phi_{AB}(P_B^{'})||\phi_{AB}(Q_B^{'})||H_{SB})$

and sends ID_S, H_{SA}, C_3 to Alice, ID_S, H_{SB}, C_4 to Bob.

Otherwise, S terminates this request.

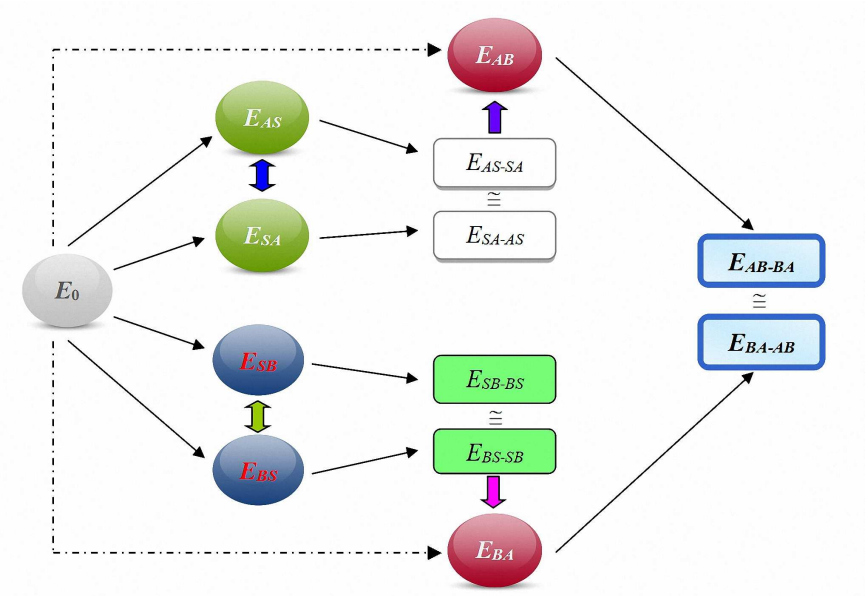

FIGURE 2. Illustration of design ideas and elliptic curves isogenies-maps

Round 5 After receiving the messages ID_S, H_{SA}, C_3, Alice firstly decrypts C_3 to $ID_A||ID_B||ID_S||E_{BA}||\phi_{BA}(P_A^{'})||\phi_{BA}(Q_A^{'})||H_{SA}$ get the messages.

Alice computes $h(ID_A||ID_B||ID_S||E_{BA}||\phi_{BA}(P_A^{'})||\phi_{BA}(Q_A^{'})||pw_A)$ locally to verify H_{SA}. If so, Alice computes $K_{AB} = j(E_{AB-BA})$ and the session key is $SK = H(j(E_{AB-BA}))$. Otherwise, Alice terminates this request. For Bob, just doing the same things as Alice. Alice and Bob can use the SK to encrypt any message for confirming opposite side has the SK. The whole authentication and key agreement phase has three session keys: $K_{AS} = j(E_{AS-SA}) = K_{SA} = j(E_{SA-AS})$ between Alice and S, $K_{BS} = j(E_{BS-SB}) = K_{SB} = j(E_{SB-BS})$ between Bob and S, $SK = H(K_{AB}) = H(j(E_{AB-BA})) = H(K_{BA}) =$

$H(j(E_{BA-AB}))$ between Alice and Bob. Figure 2 illustrates the relationship of isogenies-maps among different elliptic curves.

4. **Security Consideration.**

4.1. **Arithmetic generation and complexity assumptions.** Arithmetic generation About any fixed choice of $l_A^{e_A}$ and $l_B^{e_B}$, it is easy to found random values of f and $p = l_A^{e_A} l_B^{e_B} . f \pm 1$, where p is prime[25, 26]. For elliptic curve isogenies-based computation is also easy according to literatures[24, 27-30].

Complexity Assumptions

Problem 4.1 *(Supersingular Isogeny (SSI) problem).* Let$\phi_A : E_0 \to E_A$ be an isogeny whose kernel is $\langle [m_A] P_A + [n_A] Q_A \rangle$, where m_A and n_A are chosen at random from $\mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$ and not both divisible by ℓ_A.Given E_A and the values $\phi_A(P_B), \phi_A(Q_B)$, find a generator R_A of $\langle [m_A] P_A + [n_A] Q_A \rangle$.

Given a generator $R_A = [m_A]P_A + [n_A]Q_A$, it's easy to solve for (m_A, n_A), since E0 has smooth order and thus extended discrete logarithms are esay in E0[29].

Problem 4.2 (Supersingular Computational Diffie-Hellman (SSCDH) problem). Let $\phi_A : E_0 \to E_A$ be an isogeny whose kernel is $\langle [m_A] P_A + [n_A] Q_A \rangle$, and Let $\phi_B : E_0 \to E_B$ be an isogeny whose kernel is $\langle [m_B] P_B + [n_B] Q_B \rangle$, where m_A and n_A (respectively m_B, n_B) are chosen at random from $\mathbb{Z} / \ell_A^{e_A}\mathbb{Z}$ (respectively $\mathbb{Z} / \ell_B^{e_B}\mathbb{Z}$) and not both divisible by ℓ_A (respectively ℓ_B). Given the curves E_A, E_B and the points $\phi_A(P_B)$, $\phi_A(Q_B)$, $\phi_B(P_A)$, $\phi_B(Q_A)$, find the j-invariant of $E_0 / \langle [m_A] P_A + [n_A] Q_A, [m_B] P_B + [n_B] Q_B \rangle$.

Problem 4.3 (Supersingular Decision Diffie-Hellman (SSDDH) problem). Given a tupe sampled with probability 1/2 from one of the following two distributions:

— (E_A, E_B, $\phi_A(P_B), \phi_A(Q_B)$, $\phi_B(P_A), \phi_B(Q_A)$, E_{AB}), where E_A, E_B, $\phi_A(P_B), \phi_A(Q_B)$, $\phi_B(P_A), \phi_B(Q_A)$ are as in the SSCDH problem and

$E_{AB} \cong E_0 / \langle [m_A] P_A + [n_A] Q_A, [m_B] P_B + [n_B] Q_B \rangle$,

— (E_A, E_B, $\phi_A(P_B), \phi_A(Q_B)$, $\phi_B(P_A), \phi_B(Q_A)$, E_C), where E_A, E_B, $\phi_A(P_B), \phi_A(Q_B)$, $\phi_B(P_A), \phi_B(Q_A)$ are as in the SSCDH problem and

$E_C \cong E_0 / \langle [m'_A] P_A + [n'_A] Q_A, [m'_B] P_B + [n'_B] Q_B \rangle$,

where m'_A, n'_A (respectively m'_B, n'_B) are chosen at random from $\mathbb{Z} / \ell_A^{e_A}\mathbb{Z}$ (respectively $\mathbb{Z} / \ell_B^{e_B}\mathbb{Z}$) and not both divisible by ℓ_A (respectively ℓ_B), determine from which distribution the triple is sampled.

4.2. **Our protocol security.** Assume there are three secure components, including the three problems *SSI, SSCDH* and *SSDDH* cannot be solved in polynomial-time by quantum computers, a secure one-way hash function and a secure symmetric encryption which both can resist quantum computers attack. Assume that the adversary has full control over the insecure channel including eavesdropping, recording, intercepting, modifying the transmitted messages. However, the adversary could neither get the secret key of the

Server S and the temporary number $(m_A, n_A), (m_A^{'}, n_A^{'})$ and $(m_B, n_B), (m_B^{'}, n_B^{'})$ by Alice and Bob chosen in the local machine nor guess the shared information pw_A and pw_B correctly. We also prove that our proposed scheme achieves the security and efficiency goals. The definitions and analysis of the security requirements will be illustrated in Appendix A, and the provable security will be given in Appendix B.

5. **Efficiency Analysis.** After all, our proposed protocol is the first practical 3PAKA scheme which is based on elliptic curve isogenies towards quantum-resistant. To the best of our knowledge, no elliptic curve isogenies-based practical three-party password-authenticated key agreement protocol without using a timestamp has been proposed, so there is no literature to contrast and we sum up our proposed protocol as show in Table 2 (Security) and Table 3 (Efficiency).

Table 2. Security of our proposed protocol

No clock synchronization	**Mutual authentication**	**Impersonation**	**Man in the middle attack**	**Replay attack**
Provided	*Provided*	*Provided*	*Provided*	*Provided*
Known key security	**Perfect forward secrecy**	**Key Compromise Impersonation**	**Data integrity**	**Quantum resistant**
Provided	*Provided*	*Provided*	*Provided*	*Provided*

Our protocol is reasonably efficient. The efficiency is measured by the following two aspects:

– Communication cost: the number of communication rounds during the execution of protocol.

– Computation cost: the computation complexity of a participant.

Table 3. Efficiency of our proposed protocol

Alice or Bob				**Server S**			
Computation cost			comp. cost	*Computation cost*			comp. cost
Hash	**Symmetric en/de cryption**	**Elliptic curve isogenies**		**Hash**	**Symmetric en/de cryption**	**Elliptic curve isogenies**	
2	2	2	2	4	4	2	2

6. **Conclusion.** We put forward the first three-party password-authenticated key agreement scheme based on elliptic curve isogenies, a secure symmetric key encryption and a secure one-way hash function towards quantum-resistant. From the Table 3, we can see easily that ours protocols computing and communication are efficient. Security of our proposed protocol is also satisfactory from the Table 2. Next we will extend the proposed protocol to high level security attributes such as fairness or entanglement and so on.

REFERENCES

[1] L. M. K. Vandersypen, M. Steffen, G. Breyta, et al., Experimental realization of sho*r* s quantum factoring algorithm using nuclear magnetic resonance, *Nature*, no. 414, pp. 883–887, 2001.

[2] X. Q. Fu, W. S. Bao, C. Zhou, Speeding up implementation for Shors factorization quantum , *Chinese Sci Bull*, vol. 55, pp. 322-327, 2010.

[3] W. Chen, Z. F. Han, X. F. Mo et al., Active phase compensation of quantum key distribution system, *Chinese Sci Bull*, vol. 53, pp. 1310–1314, 2008.

[4] G. M. Nikolopoulos, Applications of single-qubit rotations in quantum public-key cryptography, *Phys Rev A*, vol. 77, pp. 032–348, 2008.

[5] D. Gottesman, I. L. Chuang., Quantum digital signatures, *arXiv: quant-ph/*0105032.

[6] T. Okamoto, K. Tanaka, S. Uchiyama. Quantum public-key cryptosystems , *Advances in Cryptology: Crypto 2000 Proceedings*, Berlin Springer, vol. 1880, pp. 147–165, 2000.

[7] A. Kawachi, T Koshiba, H. Nishimura et al., Computational indistinguishability between quantum states and its cryptographic application, *Advances in Cryptology: Eurocrypt 2005 Proceedings. Berlin: Springer,* vol. 3494, pp. 268–284, 2005.

[8] L. Yang., Quantum public-key cryptosystem based on classical NP-complete problem , *arXiv: quant-ph* /0310076.

[9] T. Koshiba., Security notions for quantum public-key cryptography, *arXiv: quant-ph/*0702183.

[10] C. Lee, C. Hsu, A secure biometric-based remote user authentication with key agreement scheme using extended chaotic maps, *Nonlinear Dyn*, vol. 71, pp. 201-211, 2013.

[11] C. Guo, C. C. Chang, Chaotic maps-based password-authenticated key agreement using smart cards, *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, pp. 1433–1440, June 2013.

[12] C. Lee, C. Li, C. Hsu, A three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps, *Nonlinear Dyn*, vol. 73, pp. 125-132, 2013.

[13] Qi Xie, Jianmin Zhao, Xiuyuan Yu, Chaotic maps-based three-party password-authenticated key agreement scheme, *Nonlinear Dyn*, vol. 74, pp. 1021-1027. doi 10.1007/s11071-013-1020-7, 2013.

[14] C. Guo, C. C. Chang, and C.Y. Sun, Chaotic Maps-Based Mutual Authentication and Key Agreement using Smart Cards for Wireless Communications , *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, no. 2, pp. 99–109, April 2013.

[15] H. Y. Lin, Improved chaotic maps-based password-authenticated key agreement using smart cards, *Com-mun. Nonlinear Sci. Numer. Simul*, vol. 20, no. 2 pp. 482 - 488, 2015.

[16] M. Dehkordi, R. Alimoradi, Identity-based multiple key agreement scheme, *KSII Transactions on Internet and Information Systems*, vol. 5, no. 12, pp. 2392-2402, December, 2011.

[17] J. Yang, T. Cao, Provably secure three-party password authenticated key exchange protocol in the standard model, *J. Syst. Softw*, vol. 85, pp. 340350, 2012.

[18] M. H. Zheng, H. H. Zhou, J. Li, G. H. Cui, Efficient and provably secure password-based group key agreement protocol, *Computer Standards & Interfaces*, vol. 31(5), pp. 948-53, 2009.

[19] L. Hui, W. Chuan-Kun, S. Jun, A general compiler for password-authenticated group key exchange protocol, *Information Processing Letters*, vol. 110, pp. 160167, 2010.

[20] L. Tian-hua, W. Qian, Z. Hong-feng, A Multi-function Password Mutual Authentication Key Agreement Scheme with privacy preserving, *Journal of information hiding and multimedia signal processing,* vol. 5, no. 2, 2014.

[21] J. Shen, Y. Du, Improving the Password-Based Authentication against Smart Card Security Breach, *Journal of Software*, vol. 8, no. 4, pp. 979-986, 2013.

[22] J. V*e*′ lu, ≪ Isog*e*′ nies entre courbes elliptiques ≫, *C.R. Acad. Sc. Paris, Se*′*rie A.*, vol. 273 pp. 238-241, 1971.

[23] J. David and D. F. Luca, Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies , *Post-Quantum Cryptography Lecture Notes in Computer Science,* vol. 7071, pp. 19-34, 2011.

[24] Alin Bostan, Francois Morain, Bruno Salvy, and eric Schost, Fast algorithms for computing isogenies between elliptic curves, *Math. Comp.*, vol. 77(263), pp. 1755-1778, 2008.

[25] Reinier Bro^{-} ker, Constructing supersingular elliptic curves, *J. Comb. Number Theory*, vol. 1(3), pp. 269-273, 2009.

[26] Jeffrey C. Lagarias and Andrew M. Odlyzko, Effective versions of the Chebotarev density theorem, *In Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, Academic Press, London*, pp. 409-464, 1977.

[27] C. X. Denis, E. Kristin, Lauter, and Z. Eyal, Goren, Cryptographic hash functions from expander graphs, *Journal of Cryptology*, vol. 22, pp. 93-113, 2009.
[28] L. Peter, Montgomery, Speeding the pollard and elliptic curve methods of factorization, *Mathematics of Computation*, vol. 48(177), pp. 243-264, 1987.
[29] T. Edlyn. The pohlig-hellman method generalized for group structure computation, *Journal of Symbolic Computation*, vol. 27(6), pp. 521-534, 1999.
[30] S. Anton, Reductionist security arguments for public-key cryptographic schemes based on group action, *The Norwegian Information Security Conference (NISK)*, pp.97-109, 2009.
[31] J. Kar and B. Majhi, An Efficient Password Security of Three Party Key Exchange Protocol based on ECDLP, *12th International Conference on Information Technology 2009 (ICIT2009)*, pp.75-78, 2009.
[32] J. Kar and B. Majhi, An Efficient Password Security of Multiparty Key Exchange Protocol based on ECDLP, *International Journal of Computer Science and Security (IJCSS)*, vol. 3(5), pp. 405-413, 2009.
[33] J. Katz, J.S. Shin, Modeling insider attacks on group key-exchange protocols, *Proceedings of the 12th ACM Conference on Computer and Communications SecurityCCS05, ACM* , pp. 180189, 2005.
[34] C. Arti, C.M. Bhandari, Secure direct communication based on pingpong protocol, *Quantum Inf Process*, vol. 8, pp. 347356, 2009
[35] D. Ariel, V. Lev, Practical quantum bit commitment protocol, *Quantum Inf Process*, vol. 11, pp. 769775, 2012
[36] S. Run-hua, Z. Hong, Multiparty quantum secret sharing with the pure entangled two-photon states, *Quantum Inf Process*, doi 10.1007/s11128-011-0239-9, vol. 11, pp. 161169, 2012.
[37] J. Grasha, A. Murugan, DNA based Cryptography: An Overview and Analysis, *Int. J. Emerg. Sci.*, vol. 3(1), pp. 36-42, March 2013.
[38] M. Garey, D. Johnson, Computers and Intractability, a Guide to the Theory of NP-Completeness, *New York: Freeman*, pp. 128130, 1979.
[39] C. Wolf, Multivariate quadratic polynomials in public key cryptography, *Katholieke Universiteit Leuven*, 2005.
[40] A. Shamir, Efficient signature schemes based on birational permutations, *Proceedings of Crypto*, pp. 1-12, 1993.
[41] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J Comput*, vol. 6, pp. 1484-1509, 1997.
[42] L.K. Grover, A fast quantum mechanical algorithm for database search[c], *Proc. 28th Annual ACM symposium on theory of computing(STOC), New York, ACM*, pp. 212–219, 1996.
[43] J. Aumasson, W.Meier, Analysis of multivariate hash functions , *Proceedings of ICISC 2007, LNCS, Berlin: Springer-Verlag,* vol. 4817, pp. 309–323, 2007.
[44] O. Billet, Robshaw, T.Peyrin, On building hash functions from multivariate quadratic equations, *Proceedings of ACISP 2007, LNCS, Berlin: Springer-Verlag*, vol. 4586, pp. 82-95, 2007.
[45] NIST. Plan for new cyptographic hash functions. http://www.nist.gov/hash-function/.
[46] H. Joseph, Silverman, The arithmetic of elliptic curves, *Graduate Texts in Mathematics, SpringerVerlag, New York*, vol. 106, 1992.
[47] R. Hartshorne, Algebraic Geometry , Springer-Verlag, Graduate Texts in Mathematics, vol. 52, 1977.
[48] J. Silverman, The arithmetic of elliptic curves , Springer-Verlag, *Graduate Texts in Mathematics*, vol. 106, 1986.
[49] M. Jean-Franois, La mmthode des graphes: Examples et applications, *In Proceedings of the international conference on class numbers and fundamental units of algebraic numbers*, pp. 217–242, 1986.
[50] D.G. Steven, Constructing isogenies between elliptic curves over finite fields, *LMS J.Comput. Math.*, vol. 2, pp. 118–138 , 1999.
[51] S.Anton, Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves, A*dv. Math. Commun.*, vol. 4(2), pp. 215–235, 2010.
[52] D.G. Steven and S. Anton, Improved algorithm for the isogeny problem for ordinary elliptic curves, *http://arxiv.org/abs/ 1105.6331/*, 2011.
[53] D.G. Steven, H. Florian, and P. Nigel, Smart Extending the GHS Weil descent attack, *Advances in cryptology-EUROCRYPT 2002 (Amsterdam), Berlin, Springer*, vol. 2332, pp. 29–44, 2002.
[54] C. Andrew, J. David, and S. Vladimir, Constructing elliptic curve isogenies in quantum subexponential time, *http://arxiv.org/abs/10124019/*, 2010.
[55] S. Wiesner, Conjugate coding, *ACM Sigact News*, vol. 15(1), pp. 78-88, 1983.

[56] MagiQ. http://www.magiqtech.com/
[57] id Quantique. http://www.idquantique.com/
[58] Toshiba-QIG. http://www.toshiba-europe.com/research/crl/QIG/
[59] C.H. Bennett, G. Brassard, Quantum cryptography: public-key distribution and coin tossing , *Proceedings IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, IEEE, New York*, pp. 175-179, 1984.
[60] C.H. Bennett, Quantum cryptography using any two nonorthogonal states, *Phys. Rev. Lett.* vol. 68, no. 3121, 1992.
[61] D. Bruss, Optimal eavesdropping in quantum cryptography with six states, *Phys. Rev. Lett.* vol.81, no.3018, 1998.
[62] A. Cabello, Quantum key distribution in the Holevo limit, *Phys. Rev. Lett.* vol. 85, no. 5635, 2000.
[63] M. Bourennane, A. Karlson, G. Bjork, Quantum key distribution using multilevel encoding , *Phys. Rev. A 64*, 012306, 2001.
[64] N. Gisin, G.Ribordy, W. Tittel, H. Zbinden, Quantum cryptography, Rev.Mod. Phys, vol. 74, no. 145, 2002.
[65] A.Beige, B.G. Engler, C. Kutrsiefer, H. Weinfurter, Secure communication with a publicly known key, *Acta. Phys. Pol. A 101*, vol. 357, 2002.
[66] S. Bose, V.Vedral, P.L. Knight, A multiparticle generalization of entanglement swapping, *Phys. Rev. A 57,* vol.822, 1998.
[67] M. Garey, D. Johnson, Computers and intractability , *A guide to the theory of NP-completeness, New York: Freeman*, pp. 128-130, 1979.
[68] J. Patarin, L. Goubin, N. Courtois, Improved Algorithms for Isomorphisms of Polynomials, *Proceedings of EURCRYPT 1998*, Berlin: Springer-Verlag, pp. 184–200, 1998.
[69] R.C. Merkle, A certified digital signature, *Proceedings of CRYPTO 1989, LNCS*, Berlin: Springer-Verlag, vol. 435, pp. 218-238, 1989.
[70] R. McEliece, A public key cryptosystem based on algebraic coding theory, *DSN progress report*, vol.42, pp. 114-116, 1978.
[71] J. Hoffstein, J. Pipher, J.H. Silverman, NSS: An NTRU Lattice-Based Signature Scheme , *Proceedings of ENCRYPT 2001, LNCS, Berlin: Springer-Verlag*, vol. 2045, pp. 211–228, 2001.
[72] C. Ran and K. Hugo, Analysis of key-exchange protocols and their use for building secure channels, *Birgit Ptzmann, editor, EUROCRYPT, Lecture Notes in Computer Science, Springer*, vol. 2045, pp. 453–474, 2001.
[73] T.Y. Wu and Y.M. Tseng, An efficient user authentication and key exchange protocol for mobile client-server environments, *Computer Networks*, vol. 54 (9), pp. 1520–1530, 2010.
[74] T. Y. Wu and Y. M. Tseng, An ID-based mutual authentication and key exchange protocol for low-power mobile devices, *The Computer Journal*, vol. 53(7), pp. 1062–1070, 2010.

Appendix A. The definitions and analysis of our scheme

No clock synchronization

Theorem A.0. *The proposed protocol need not clock synchronization.*

The proposed protocol solves the clock synchronization problem with no timestamp mechanism. Instead, we introduce fresh random number (m_A, n_A), $(m_A^{'}, n_A^{'})$ and (m_B, n_B), $(m_B^{'}, n_B^{'})$ to provide the challenge response security mechanism so that replay attack cannot threaten the proposed scheme while no clock synchronization is needed.

Mutual authentication and key agreement

Definition A.1. Mutual authentication and key agreement refers to two parties authenticating each other suitably and getting the session key simultaneously.

Theorem A.1. *The proposed protocol can achieve mutual authentication and key agreement.*

Proof. The proposed scheme allows Alice to authenticate the server S by checking whether $h(ID_A||ID_B||ID_S||E_{BA}||\phi_{BA}(P_A^{'})||\phi_{BA}(Q_A^{'})||pw_A) \stackrel{?}{=} H_{SA}$. Because only S can compute H_{SA} by shared information pw_A and own secret keys (m_S, n_S). The same process will happen for Bob to authenticate S. The server S authenticates Alice or Bob by compuing $H_A^{'} \stackrel{?}{=} H_A$ or $H_B^{'} \stackrel{?}{=} H_B$, because only Alice or Bob holds the shared information

pw_A or pw_B except S. After Alice or Bob authenticates S, she or he will get the secret information to compute the fresh session key between Alice and Bob locally based on the temporary $(m_A^{'}, n_A^{'})$ and $(m_B^{'}, n_B^{'})$.

Resist well-known attacks

(1) Impersonation attack/Man-in-the-middle attack

Definition A.2. An impersonation attack is an attack in which an adversary successfully assumes the identity of one of the legitimate parties in a system or in a communications protocol.

Definition A.3. The man-in-the-middle attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker

Theorem A.2. *The proposed protocol can resist impersonation attack.*

Theorem A.3. *The proposed protocol can resist Man-in-the-middle attack.*

Proof. An adversary cannot impersonate Alice to cheat the server S, because it is not able to structure the message $h(ID_A||ID_B||ID_S||E_{AB}||\phi_{AB}(P_B^{'})||\phi_{AB}(Q_B^{'})||pw_A)$ without the knowledge of the shared password. It either cannot masquerade as the server S to cheat Alice or Bob without the knowledge of the shared password and the the secret key of the Server S.

On the other hand, because each interaction messages in our protocol contains the users' identities, a man-in-the-middle attack cannot succeed.

Remark. A password setup algorithm is another problem and we need not handle it in this paper.

(2) Replay attack

Definition A.4. A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.

Theorem A.4. *The proposed protocol can resist replay attack.*

Proof. An adversary cannot start a replay attack against our scheme because of the freshness of $(m_A^{'}, n_A^{'})$ and $(m_B^{'}, n_B^{'})$ in each session. If $(P_A^{'}, Q_A^{'}), (P_B^{'}, Q_B^{'})$ has appeared before or the status shows in process, Alice or Bob rejects the session request. If the adversary wants to launch the replay attack successfully, it must compute and modify $C_i (1 \leq i \leq 4)$ correctly which is impossible according to *SSCDH* and *SSDDH problems*.

(3) Known-key security

Definition A.5. A protocol can protect the subsequent session keys from disclosing even if the previous session keys are revealed by the intendant user is called known-key security.

Theorem A.5. *The proposed protocol can achieve known-key security.*

Proof. Since the session key $SK = H(j(E_{AB-BA}))$ is depended on the invariant j of elliptic curve E_{AB-BA} which is generated by random nonces $(m_A^{'}, n_A^{'})$ and $(m_B^{'}, n_B^{'})$, bases $(P_A^{'}, Q_A^{'})$ and $(P_B^{'}, Q_B^{'})$, and E_0. Because the generation of nonces is independent in all sessions, an adversary cannot compute the previous and the future session keys when he knows one session key unless he can solve *SSCDH* and *SSDDH problems*.

(4) Perfect forward secrecy

Definition A.6. An authenticated multiple key establishment protocol provides perfect forward secrecy if the compromise of both the node's secret keys cannot results in the compromise of previously established session keys [31] [32]**.**

Theorem A.6. *The proposed protocol can achieve perfect forward secrecy.*

Proof. In the proposed scheme, the session key $SK = H(j(E_{AB-BA}))$ is related with $(m_A^{'}, n_A^{'})$ and $(m_B^{'}, n_B^{'})$, which were chosen by Alice and Bob, respectively. Because of

the intractability of the *SSCDH* and *SSDDH problems*, an adversary cannot compute the previously established session keys.

(5) Key Compromise Impersonation Attacks (KCI attacks)

Definition A.7. Informally, an adversary is said to impersonate a party B to another party A if B is honest and the protocol instance at A accepts the session with B as one of the session peers but there exists no such partnered instance at B [33]. In a successful KCI attack, an adversary with the knowledge of the long-term private key of a party A can impersonate B to A.

Theorem A.7. *The proposed protocol can resist* KCI *attack.*

Proof. We assume that an adversary can know Alice's password pw_A (the adversary may be Alice's close friend), then he wants to impersonate Bob to cheat Alice. But the attack process will not achieve and the attack course terminates. Because an adversary can't own the Bob's password pw_A, and he can't compute $h(ID_A||ID_B||ID_S||E_{BA}||\phi_{BA}(P_A^{'})||\phi_{BA}(Q_A^{'})||pw_B)$. The trust server S will check if $H_A^{'} \stackrel{?}{=} h(ID_A||ID_B||ID_S||E_{BA}||\phi_{BA}(P_A^{'})||\phi_{BA}(Q_A^{'})||pw_B)$. If not, server S terminates it. So key compromise impersonation attacks fails.

(6) Data integrity

Definition A.8. Authentication key establishment protocol is said to achieve the property of data integrity, if there is no polynomial time algorithm that can alter or manipulate the transmitted messages.

Theorem A.8. *The proposed protocol can achieve data integrity property.*

Proof. While the Alice sends the sensitive data to the server S by the communication channel, the adversary alter or manipulate the data and cheat the trust server S by relying the wrong session keys. If the adversary wants to alter or manipulate the messages $\{(P_A, Q_A), ID_A, E_{AS}, \phi_{AS}(P_S), \phi_{AS}(Q_S)\}$ of **Round 1** for cheating S, and he will be detected in the **Round 4**. Because the adversary has not Alice's password pw_A, then he can not compute the $h(ID_A||ID_B||ID_S||E_{AB}||\phi_{AB}(P_B^{'})||\phi_{AB}(Q_B^{'})||pw_A)$. If the adversary wants to alter or manipulate the messages $\{(P_A^{'}, Q_A^{'}), (P_B^{'}, Q_B^{'}), ID_S, E_{SA}, \phi_S(P_A), \phi_S(Q_A)\}$ of **Round 2** for cheating Alice, and he will be detected in the **Round 3**. Because the adversary has not the secret key of server S and Alice's password pw_A, then he can not compute $h(ID_A||ID_B||ID_S||E_{BA}||\phi_{BA}(P_A^{'})||\phi_{BA}(Q_A^{'})||pw_A)$

(7) Quantum resistant

Definition A.9. It encompasses all the ways in which can resist quantum computer attack, including quantum cryptography [34-36], DNA cryptography[37] and resistance to quantum algorithms [23, 38-40], and we called them Post-Quantum Cryptography or Quantum Resistant Cryptography.

Theorem A.9. *The proposed protocol can resist quantum computer attack.*

Proof. Our proposed protocol is composed of three parts: elliptic curve isogenies in Public Key Cryptosystem, a secure one-way hash function and a pair of secure symmetric encryption/decryption which all can resist quantum computer attack. **(a) Elliptic curve isogenies algorithm.** The Shor algorithm [41] is the greatest threat which can attack most public key Cryptosystem, such as RSA, Diffie-Hellman, ELGamal and ECC. Theory indicates that 256 bits elliptic curve cryptography can be decoded by 1024 bits quantum computer, and 1024 bits RSA cryptography can be cracked by 2048 bits quantum computer easily. However, our protocol adopts elliptic curve isogenies in public key Cryptosystem which can resist quantum computers, even for quantum computers attack that still requires fully exponential time [23]. Recently, Stolbunov [51] proposed a Diffie-Hellman type system based on the difficulty of computing isogenies between ordinary

elliptic curves, with the stated aim of obtaining quantum-resistant cryptographic protocols. The fastest known (classical) probabilistic algorithm for solving this problem is the algorithm of Galbraith and Stolbunov [52], based on the algorithm of Galbraith, Hess, and Smart [53]. This algorithm is exponential, with a worst-case running time of $O(\sqrt[4]{q})$. However, on a quantum computer, recent work of Childs et al. [54] has shown that the private keys in Stolbunov's system can be recovered in subexponential time. Moreover, even if we only consider classical attacks in assessing security levels, Stolbunov's scheme requires 229 seconds (even with precomputation) to perform a single key exchange operation at the 128-bit security level on a desktop PC [51]. **(b) A pair of secure symmetric algorithm.** Anyway, Grover algorithm [42] is the general method which can reduce the key length to half for symmetric cryptography. So we can double the key length and adopt a secure symmetric algorithm, that is enough. **(c) A secure one-way hash function**. Until now many multivariate hash functions can resist quantum computers attack, such as [43-45] and so on.

A. **Appendix B. The provable security of our scheme.** We recall the definition of session-key security in the authenticated-links adversarial model of Canetti and Krawczyk [72]. The basic descriptions are shown in Table 4.

Table 4. Descriptions the model of Canetti and Krawczyk

Symbol	Definition
parties P_1, P_n	Modeled by probabilistic Turing machines.
Adversary Λ	A probabilistic Turing machine which controls all communication, with the exception that the adversary cannot inject or modify messages (except for messages from corrupted parties or sessions), and any message may be delivered at most once.
Send query	The adversary can control over Parties outgoing messages via the **Send** query. Parties can be activated by the adversary launching **Send** queries.
Two sessions matching	If the outgoing messages of one session are the incoming messages of the other

We allow the adversary access to the queries **SessionStateReveal**, **SessionKeyReveal**, and **Corrupt**.
(1) **SessionStateReveal(*s*)**: This query allows the adversary to obtain the contents of the session state, including any secret information. ***s*** means no further output.
(2) **SessionKeyReveal(*s*)**: This query enables the adversary to obtain the session key for the specified session ***s***, so long as ***s*** holds a session key.
(3) **Corrupt(P_i)** : This query allows the adversary to take over the party P_i , including long-lived keys and any session-specific information in P_i's memory. A corrupted party produces no further output.
(4) **Test(*s*)**: This query allows the adversary to be issued at any stage to a completed, fresh, unexpired session ***s***. A bit b is then picked randomly. If $b = 0$, the test oracle reveals the session key, and if $b = 1$, it generates a random value in the key space. The adversary Λ can then continue to issue queries as desired, with the exception that it cannot expose the test session. At any point, the adversary can try to guess b. Let $GoodGuess^{\Lambda}(k)$ be the event that the adversary Λ correctly guesses b, and we define the advantage of adversary Λ as $Advantage^{\Lambda}(k) = \max\{0, |\Pr[GoodGuess^{\Lambda}(k)] - \frac{1}{2}|\}$, where k is a security parameter.

A session s is locally exposed with P_i: if the adversary has issued **SessionStateReveal(s)**, **SessionKeyReveal(s)**, **Corrupt(P_i)** before s is expired.

Definition B.1. A key exchange protocol Π_1 in security parameter k is said to be session-key secure in the authenticated-links adversarial model of Canetti and Krawczyk if for any polynomial-time adversary Λ,

Algorithm 1 SSDDH distinguisher

Input: $E_A, E_B, \phi_A(P_B), \phi_A(Q_B), \phi_B(P_A), \phi_B(Q_A), E$

1: $r \xleftarrow{R} \{1,...,k\}$, where k is an upper bound on the number of sessions activated by Λ in any interaction.

2: Invoke Λ and simulate the protocol to Λ, except for the $r-th$ activated protocol session.

3: For the $r-th$ session, let Alice send $A, i, E_A, \phi_A(P_B), \phi_A(Q_B)$ to Bob, and let Bob send $B, i, E_B, \phi_B(P_A), \phi_B(Q_A)$ to Alice, where i is the session identifier. Both Alice and Bob can compute $E_{AB} = \phi_B'(\phi_A(E_0)) = \phi_A'(\phi_B(E_0)) = E_0 / \langle [m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B \rangle$ locally.

4: **if** the $r-th$ session is chosen by Λ as the test session **then**

5: Provide Λ as the answer to the test query.

6: $d \leftarrow \Lambda$'s output.

7: **else**

8: $d \xleftarrow{R} \{0,1\}$.

9: **end if**

Output: d

(1.) If two uncorrupted parties have completed matching sessions, these sessions produce the same key as output;

(2.) $Advantage^{\Lambda}(k)$ is negligible.

Theorem B.1. *Under the SSDDH assumption, using the Algorithm 1 to compute session key is session-key secure in the authenticated-links adversarial model of Canetti and Krawczyk* [72].

Proof. The proof is based on the proof given by Refs. [23,30,72]. There are two uncorrupted parties in matching sessions output the same session key, and thus the first part of Definition B.1 is satisfied. To show that the second part of the definition is satisfied, assume that there is a polynomial-time adversary with a non-negligible advantage ε in standard model. We claim that Algorithm 1 forms a polynomial-time distinguisher for SSDDH having non-negligible advantage.

Probability analysis. It is clear that Algorithm 1 runs in polynomial time and has non-negligible advantage. There are two cases where the r-th session is chosen by Λ as the test session: (1) If the r-th session is not the test session, then Algorithm 1 outputs a random bit, and thus its advantage in solving the SSDDH is 0. (2) If the r-th session is the test session, then Λ will succeed with advantage ε, since the simulated protocol provided to Λ is indistinguishable from the real protocol. The latter case occurs with probability $1/k$, so the overall advantage of the SSDDH distinguisher is ε/k, which is non-negligible.

Definition B.2. A key exchange protocol in security parameter k is said to be session-key secure in the adversarial model of Canetti and Krawczyk if for any polynomial-time adversary Λ,

Algorithm 2 SSDDH distinguisher with authenticated parameter

Input: $E_A, E_B, \phi_A(P_B), \phi_A(Q_B), \phi_B(P_A), \phi_B(Q_A), E, H$

1: $r \xleftarrow{R} \{1,...,k\}$, where k is an upper bound on the number of sessions activated by Λ in any interaction.
2: Invoke Λ and simulate the protocol to Λ, except for the $r-th$ activated protocol session.
3: For the $r-th$ session, let Alice send $A, i, E_A, \phi_A(P_B), \phi_A(Q_B)$ to Bob, and let Bob send $B, i, E_B, \phi_B(P_A), \phi_B(Q_A)$ to Alice, where i is the session identifier. Both Alice and Bob can compute $E_{AB} = \phi_B'(\phi_A(E_0)) = \phi_A'(\phi_B(E_0)) = E_0 / \langle [m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B \rangle$ locally, and then use the common j-invariant of above equation to form a secret shared key which encrypt authenticated information.
4: **if** the $r-th$ session is chosen by Λ as the test session **then**
5: Provide Λ as the answer to the test query.
6: $d \leftarrow \Lambda$'s output.
7: **else**
8: $d \xleftarrow{R} \{0,1\}$.
9: **end if**
Output: d

(3.) If two uncorrupted parties have completed matching sessions with pre-distributed parameter, these sessions produce the same key as output;

(4.) $Advantage^{\Lambda}(k)$ is negligible.

Theorem B.2. *Under the SSDDH assumption, using the Algorithm 2 to compute session key is session-key secure in the adversarial model of Canetti and Krawczyk* [72].

Proof. The proof's process is similar to **Theorem B.1**. The only difference between protocol $\Pi_1$and Π_2 is that the protocol Π_2 using session key to encrypt the authenticated information. Since **Theorem B.1** is session-key secure, the protocol Π_2 is also session-key secure.

Probability analysis. It is similar to Algorithm 1. If we assume that Algorithm 2 forms a polynomial-time distinguisher for SSDDH having non-negligible advantage, the overall advantage of the SSDDH distinguisher with authenticated parameter is , which is also non-negligible.

Definition B.3. A composable key exchange protocol Π_3 in security parameter k is said to be session-key secure in the adversarial model of Canetti and Krawczyk if for any polynomial-time adversary Λ,

Algorithm 3 Proposed protocol simulator

Input: $ID_A, ID_B, ID_C, H, E_0, (P_S, Q_S)$

1: $r \xleftarrow{R} \{1,...,k\}$, where k is an upper bound on the number of sessios activated by Λ in any interaction.

2: Invoke Λ and simulate the protocol to Λ, except for the $r-th$ activated protocol session.

3: For the $r-th$ session, let Alice run the protocol Π_2 with the trust server, and and let Bob run the protocol Π_2 with the trust server. After the trust server authenticate Alice and Bob, the trust server runs the protocol Π_1 with Alice and Bob respectively.

4: **if** the $r-th$ session is chosen by Λ as the test session **then**

5: Provide Λ as the answer to the test query.

6: $d \leftarrow \Lambda'$s output.

7:**else**

8: $d \xleftarrow{R} \{0,1\}$.

9:**end if**

Output: d

(5.) If two uncorrupted parties have completed matching sessions with pre-distributed parameter, these sessions produce the same key as output;

(6.) $Advantage^{\Lambda}(k)$ is negligible.

Theorem B.3. *Under the SSDDH assumption, using the Algorithm 3 to compute session key is session-key secure in the adversarial model of Canetti and Krawczyk* [72].

Proof. The proof's process is similar to Theorem B.1. The protocol Π_3 is the composable instance of protocol Π_1 and Π_2. The protocol Π_3 uses $\Pi_2$to make trust server authenticate the two-party and transfer the secret parameters to help Alice and Bob to run protocol Π_1 to get the session key which can't be compute by any other parties except for Alice and Bob. Since Theorem B.1 and Theorem B.2 are session-key secure, the protocol Π_3 is also session-key secure.

Probability analysis. It is similar to Algorithm 1. If we assume that Algorithm 3 forms a polynomial-time distinguisher for SSDDH having non-negligible advantage, the overall advantage of the proposed protocol simulator with authenticated parameter is ε/k which is also non-negligible. Because the protocol Π_3 chooses different parameters to structure session keys in different phase which are secure independence of protocol Π_1 and Π_2.