Password-Based Authenticated Key Exchange from Standard Isogeny Assumptions

Shintaro Terada and Kazuki Yoneyama(✉)

Ibaraki University, 4-12-1, Nakanarusawa, Hitachi-shi, Ibaraki, Japan
kazuki.yoneyama.sec@vc.ibaraki.ac.jp

Abstract. The isogeny-based cryptosystems are considered as one of post-quantum cryptosystems. Taraskin et al. proposed a password-based authenticated key exchange (PAKE) scheme from isogeny by extending Jao et al.'s supersingular isogeny Diffie-Hellman (SIDH) protocol. In their scheme, a new group action is introduced in addition to SIDH due to non-commutativity of SIDH in order to embed the password to the DH public key. Also, in the security proof, new non-standard assumptions regarding the new group action are necessary. It is not clear if these assumptions are really hard.

In this paper, we propose new PAKE schemes, SIDH-EKE and CSIDH-EKE, which are secure under the standard assumptions (corresponding to the computational DH assumption). Our schemes are obtained by a combination of SIDH (or CSIDH, commutative SIDH) and EKE (encrypted key exchange). We prove security of our schemes under the same standard assumptions as original SIDH and CSIDH in the random oracle model and ideal cipher model. CSIDH-EKE achieves more compact communication overhead than Taraskin et al.'s scheme.

Keywords: Authenticated key exchange · Password-based authenticated key exchange · Isogeny-based cryposystems

1 Introduction

1.1 Backgrounds

Post-quantum cryptosystems (PQC) are one of hottest research topics in cryptography due to emerging of quantum computers. Though the most studied PQC is lattice-based, other alternatives are also required to risk diversification as NIST's PQC standardization [1]. Isogeny-based cryptosystems are one of candidates of PQC. Given two elliptic curves $E, E'/\mathbb{F}_p$, non-zero homomorphism $\psi : E \to E'$ is called an isogeny. By Vélu's formula [39], given elliptic curve E and point R, we can efficiently compute an isogeny $\psi : E \to E/\langle R \rangle$ with kernel $\langle R \rangle$.

R. Steinfeld and T. H. Yuen (Eds.): ProvSec 2019, LNCS 11821, pp. 41–56, 2019.
https://doi.org/10.1007/978-3-030-31919-9_3

On the other hand, given two isogenous elliptic curves E and E', to find a (compact representation of) isogeny $\psi : E \to E'$ (the isogeny computation problem) is believed to be hard even for quantum computers. Isogeny-based cryptosystems rely on the isogeny computation problem and its derivations. The advantage of isogeny-based cryptosystems against other PQC candidates is compactness of the key size and the ciphertext size.

Couveignes [13] initiated the research of isogeny-based cryptography by formulating the basic notion of *hard homogeneous spaces (HHSs)* which is an abstract form of isogeny graphs and class groups of endomorphism rings of (ordinary) elliptic curves. Rostovtsev and Stolbunov [37] proposed a DH type key exchange scheme from ordinary elliptic curve isogenies. On the other hand, Childs et al. [12] showed that the isogeny computation problem on ordinary elliptic curve isogenies can be analysed in quantum subexponential time. Then, Jao et al. [16,25] proposed supersingular isogeny-based DH type key exchange (SIDH) scheme because no quantum subexponential time analysis is known for the isogeny computation problem on supersingular elliptic curve isogenies. It is known that j-invariants $j(E) = j(E')$ (where $j(E)$ is deterministically derived from E) iff elliptic curves E and E' are isomorphic. SIDH uses this property to share j-invariants as the common session key between parties. Also, Castryck et al. [11] proposed a new HHS-based key exchange scheme called *CSIDH (commutative SIDH)*, which is constructed from a group action on the set of supersingular elliptic curves defined over a prime field. Since the group action is commutative in CSIDH, we can deal with it as a similar manner to classical DH key exchange. In CSIDH, a common secret curve is obtained between parties resulting from the group action, and the Montgomery coefficient of the curve is shared as the common session key. Moreover, validity of public keys can be efficiently verified while SIDH has no efficient method yet. Hence, CSIDH is very compatible to classical DH.

There is a trade-off between the SIDH system and the CSIDH system. The advantage of SIDH is that computational time is relatively faster than the CSIDH while it is slower than other PQC candidates. For the security level corresponding to 64 bit quantum security and 128 bit classical security (i.e., NIST category 1 [1]), computational time for the SIDH key exchange is about 10 times faster than the CSIDH key exchange. On the other hand, the advantage of CSIDH is that the key size is more compact than SIDH while the key size of SIDH is also more compact than other PQC candidates. For the parameter of NIST category 1, the key size is about one fifth of these of SIDH. Also, another major advantage of CSIDH is efficient puiblic key validation.

Since SIDH and CSIDH are only secure against passive (i.e., just eavesdropping) adversaries, authenticated key exchange (AKE) schemes [18,19,33,34,40] from isogeny have been recently studied. AKE schemes aim to ensure security against active adversaries such as impersonation resilience, known-key security, and forward secrecy. In AKE, each party has a pre-established static secret key as the credential, and publishes the corresponding static public key. Thus, some public key infrastructure (PKI) is necessary.

On the other hand, in the real world, the most popular authentication mechanism is the password authentication. Hence, password-based authenticated key exchange (PAKE) is important to study in a practical sense. In PAKE, parties shares a human-memorable password in advance, they do not need any PKI. Since passwords are chosen from a small dictionary, we must consider online and off-line dictionary attacks as well as security of AKE. Many PAKE schemes based on the classical DH key exchange have been introduced such as [3,5,9,10,20,21,23,26–30,32,35]. Taraskin et al. [38] introduced the first PAKE scheme (TSJL scheme) from isogeny. The TSJL scheme is an extension of SIDH to password-based. The construction idea is simple: each party encodes the password to SIDH public key, and decodes the received public key with the password. To achieve such an encoding, they proposed a new group action. Also, security of the TSJL scheme is proved in the Bellare-Pointcheval-Rogaway (BPR) model under new assumptions related to the new group action in the random oracle (RO) model. However, in [38], justification of new assumptions is not sufficiently discussed. Thus, it is desirable to construct a PAKE scheme based on a standard isogeny problem.

1.2 Our Contribution

We propose two new PAKE schemes from isogeny, called SIDH-EKE and CSIDH-EKE, which are secure under the standard isogeny assumptions. Our main idea is to compose SIDH (or CSIDH) and encrypted key exchange (EKE) [4]. EKE is a PAKE scheme based on classical DH key exchange, and security is proved in [3] as EKE2. Each party encrypts the DH public key with the password as the key, and decrypts the received ciphertext with the password. The session key is generated by hashing the session key of the classical DH key exchange with session-specific information. In (C)SIDH-EKE, each party encrypts the (C)SIDH public key with the password, and decrypts the received ciphertext with the password. By the same way as (C)SIDH, the key material of the session key can be generated, and the session key is the hashed value of the key material and session-specific information. The computational cost and the communication cost is almost the same as (C)SIDH. We prove that (C)SIDH-EKE is secure in the BPR model under the standard (C)SIDH assumption (i.e., corresponding to the classical computational DH assumption) in the RO model and the ideal cipher (IC) model. The security proof follows the proof of EKE. However, since algebraic structures are different between (C)SIDH-EKE and EKE, we cannot directly use the proof strategy of EKE. Hence, we give the modification of the proof of EKE according to the algebraic structure of (C)SIDH by using the hybrid argument.

The advantage of our SIDH-EKE against the previous PAKE scheme from isogeny (i.e., the TSJL scheme) is that SIDH-EKE can be proved under the standard SIDH assumption while the TSJL scheme is proved under non-standard assumptions. The advantage of our CSIDH-EKE against the TSJL scheme is communication overhead. Though the TSJL scheme (and SIDH-EKE) need 2640 bit overhead for each party, CSIDH-EKE only needs 512 bit overhead for the

same security level (NIST category 1)[1] in exchange for the computational cost. The detailed efficiency comparison is given in Table 1.

1.3 Related Work

Many post-quantum key exchange schemes have been studied. Fujioka et al. [17] proposed a generic construction of AKE from KEM, and showed instantiations from lattices and codes. Ding et al. [15] proposed an AKE schemes from the Learning with Errors (LWE) problem and the Ring-LWE (RLWE) problem. Bos et al. [8] proposed an RLWE-based AKE scheme for TLS, and Alkim et al. [2] improved it as NewHope. Also, Bos et al. [7] proposed a LWE-based AKE scheme, Frodo.

On the other hand, there are few post-quantum PAKE schemes. Katz and Vaikuntanathan [31] proposed the first PAKE scheme based on lattices. To remove noise from the shared session key, their scheme uses an error-correcting code; and thus, it needs three moves. Ding et al. [14] proposed RLWE-based PAKE schemes. One guarantees explicit authentication with three moves, and the other needs two moves (not one-round). Generally, isogeny cryptosystem is advantageous to lattice cryptosystem in key sizes. Hence, (C)SIDH-EKE can be implemented by smaller key sizes than these lattice-based PAKE schemes. Also, (C)SIDH-EKE can be executed in one-round (i.e., parties can exchange public keys simultaneously) while known lattice-based PAKE schemes are not.

2 Preliminaries

In this section, we recall SIDH, HHS, CSIDH, EKE and the BPR model.

Throughout this paper we use the following notations. If M is a set, then by $m \in_R \mathsf{M}$ we denote that m is sampled randomly from M. If $\mathcal{R}$ is an algorithm, then by $y \leftarrow \mathcal{R}(x;r)$ we denote that y is output by $\mathcal{R}$ on input x and randomness r (if $\mathcal{R}$ is deterministic, r is empty). The security parameter is λ.

2.1 SIDH

Here, we recall the SIDH system [16,25].

For two small primes ℓ_A, ℓ_B (e.g., $\ell_A = 2, \ell_B = 3$), let p be a large prime such that $p \pm 1 = f \cdot \ell_A^{e_A} \ell_B^{e_B}$ for a small f and $\ell_A^{e_A} \approx \ell_B^{e_B} = 2^{\Theta(\lambda)}$. Let E over $\mathbb{F}_{p^2}$ be a random supersingular elliptic curve with $E(\mathbb{F}_{p^2}) \simeq (\mathbb{Z}/(p \pm 1)\mathbb{Z})^2 \supseteq$

[1] Very recently, Peikert [36] showed a new quantum security analysis of CSIDH-512, corresponding to NIST category 1, by using the collimation sieve technique, and CSIDH-512 is broken by 40 bit quantum memory and 2^{16} quantum oracle queries (i.e., 56 bit quantum security). Hence, He estimates that the quantum security level of CSIDH-512 is rather weaker than NIST category 1. On the other hand, the quantum circuit for the group operation of CSIDH is very high cost. Thus, by considering such external overheads of circuits in addition to his evaluation, CSIDH-512 still seems safe in reality.

$(\mathbb{Z}/\ell_A^{e_A}\mathbb{Z})^2 \oplus (\mathbb{Z}/\ell_B^{e_B}\mathbb{Z})^2$. For isogenies ψ_A and ψ_B with kernels of orders $\ell_A^{e_A}$ and $\ell_B^{e_B}$, respectively, let $\ker\psi_A = \langle R_A\rangle \subset E[\ell_A^{e_A}]$, $\ker\psi_B = \langle R_B\rangle \subset E[\ell_B^{e_B}]$, $\ker\psi_{BA} = \langle\psi_B(R_A)\rangle \subset E_B[\ell_A^{e_A}]$ and $\ker\psi_{AB} = \langle\psi_A(R_B)\rangle \subset E_A[\ell_B^{e_B}]$. Then, for $\psi_A : E \to E_A = E/\langle R_A\rangle$ and $\psi_B : E \to E_B = E/\langle R_B\rangle$, $\psi_{AB} : E_A \to E/\langle R_A, R_B\rangle$ and $\psi_{BA} : E_B \to E/\langle R_A, R_B\rangle$ hold. Thus, we can use j-invariants $j(E/\langle R_A, R_B\rangle)$ as the common secret computed by two ways. Please see [16,25] for the detail of the mathematical foundation of the SIDH system.

In the SIDH system, hardness assumptions are defined as classical DH. We recall the computational DH-type assumptions for SIDH defined in [16].

Definition 1 (SI-CDH Problem [16]). *For $a \in_R \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$, $b \in_R \mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$, $E[\ell_A^{e_A}] = \langle P_A, Q_A\rangle$, $E[\ell_B^{e_B}] = \langle P_B, Q_B\rangle$, $R_A = P_A + aQ_A$, $R_B = P_B + bQ_B$, $\psi_A : E \to E_A = E/\langle R_A\rangle$ and $\psi_B : E \to E_B = E/\langle R_B\rangle$, the advantage of a PPT solver $\mathcal{S}$ in the SI-CDH problem for public parameter $Param = (E, P_A, Q_A, P_B, Q_B)$ is defined as*

$$\mathsf{Adv}^{\mathsf{si\text{-}cdh}}_{E,\ell_A,\ell_B}(\mathcal{S}) = \Pr[\mathcal{S}(Param, (E_A, \psi_A(P_B), \psi_A(Q_B)), (E_B, \psi_B(P_A), \psi_B(Q_A))) \to j(E/\langle R_A, R_B\rangle)].$$

The SI-CDH problem corresponds to the classical computational DH problem.

Protocol of SIDH. Here, we recall the protocol of SIDH [25].

Public Parameters. Let $E[\ell_A^{e_A}] = \langle P_A, Q_A\rangle$ and $E[\ell_B^{e_B}] = \langle P_B, Q_B\rangle$. The public parameters are (E, P_A, Q_A, P_B, Q_B).

Session. Parties A and B executes a key exchange session as follows:

1. Party A chooses $a \in_R \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$, computes $R_A = P_A + aQ_A$ and $\psi_A : E \to E_A = E/\langle R_A\rangle$, and sends the public key $\hat{A} = (E_A, \psi_A(P_B), \psi_A(Q_B))$ to party B.
2. Party B chooses $b \in_R \mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$, computes $R_B = P_B + bQ_B$ and $\psi_B : E \to E_B = E/\langle R_B\rangle$, and sends the public key $\hat{B} = (E_B, \psi_B(P_A), \psi_B(Q_A))$ to party A.
3. On receiving $\hat{B}$, party A computes $R_{BA} = \psi_B(P_A) + a\psi_B(Q_A)$ and generates the session key $SK = j(E_B/\langle R_{BA}\rangle)$.
4. On receiving $\hat{A}$, party B computes $R_{AB} = \psi_A(P_B) + b\psi_A(Q_B)$ and generates the session key $SK = j(E_A/\langle R_{AB}\rangle)$.

Since $E_B/\langle R_{BA}\rangle$ and $E_A/\langle R_{AB}\rangle$ are isomorphic, $j(E_B/\langle R_{BA}\rangle) = j(E_A/\langle R_{AB}\rangle)$ holds.

It is obvious that the session key SK is hard to find for any passive adversary if the SI-CDH problem is hard.

2.2 Hard Homogeneous Space and CSIDH

Here, we recall the definition of HHS [13], and the CSIDH system [11] as an instantiation of HHS.

Definition 2 (Freeness and Transitivity). *X denotes a finite set, and G denotes an abelian group. We say that G acts efficiently on X freely and transitively if there is an efficiently computable map $* : G \times X \to X$ as follows:*

- *for any $x \in X$ and $g, h \in G$, $g * (h * x) = (gh) * x$ holds, and there is an identity element $id \in G$ such that $id * x = x$,*
- *for any $(x, y) \in X \times X$, there is $g \in G$ such that $g * x = y$, and*
- *for any $x \in X$ and $g, h \in G$ such that $g * x = h * x$, $g = h$ holds.*

Definition 3 (Hard Homogeneous Space). *A HHS consists of a finite abelian group G acting freely and transitively on some set X such that the following tasks are efficiently executable:*

- *Computing the group operation on G*
- *Sampling randomly from G with (close to) uniform distribution*
- *Deciding validity and equality of a representation of elements of X*
- *Computing the action of a group element $g \in G$ on some $x \in X$ (i.e., $g * x$)*

The CSIDH system is an instantiation of HHS from $\mathbb{F}_p$-rational supersingular elliptic curves and their $\mathbb{F}_p$-rational isogeny. Let $\mathcal{E}\ell\ell_p(\mathcal{O})$ be the set of elliptic curves over $\mathbb{F}_p$ whose $\mathbb{F}_p$-rational endomorphism ring is some fixed quadratic order $\mathcal{O}$, and $\mathrm{cl}(\mathcal{O})$ be the ideal class group of $\mathcal{O}$. Then, the CSIDH system is regarded as HHS by setting $X = \mathcal{E}\ell\ell_p(\mathcal{O})$ and $G = \mathrm{cl}(\mathcal{O})$ as the parameter of HHS. For curve $E \in X$ and ideal class $[\mathfrak{g}] \in G$, the group action $[\mathfrak{g}] * E$ corresponds to the map $([\mathfrak{g}], E) \longmapsto E/\mathfrak{g}$. Since $E/\mathfrak{g}$ is a supersingular curve, the form of $E/\mathfrak{g}$ is $y^2 = x^3 + cx^2 + x$ for $c \in \mathbb{F}_p$. Then, $[\mathfrak{g}] * E$ can be represented as such Montgomery coefficient c.

Due to commutativity of $\mathrm{cl}(\mathcal{O})$, for $[\mathfrak{g}], [\mathfrak{g}'] \in G$, $E \in X$, $E_{\mathfrak{g}} = E/\mathfrak{g}$ and $E_{\mathfrak{g}'} = E/\mathfrak{g}'$, curves $E_{\mathfrak{g}'}/\mathfrak{g}$ and $E_{\mathfrak{g}}/\mathfrak{g}'$ are identical. Thus, we can use the Montgomery coefficient of $E/\mathfrak{g}\mathfrak{g}'$ (i.e., $([\mathfrak{g}][\mathfrak{g}']) * E$) as the common secret computed by two ways. Please see [11] for the detail of the mathematical foundation of the CSIDH system. In this paper, we use the notation of HHS as the CSIDH system for simplicity.

In the CSIDH system, hardness assumptions are defined as classical DH by using HHS. We recall the computational DH-type assumption for HHS defined in [6].[2]

Definition 4 (CSI-CDH Problem [6]). *For $E_0 \in X$, $[\mathfrak{a}], [\mathfrak{b}] \in_R G$, $E_{\mathfrak{a}} = [\mathfrak{a}] * E_0$ and $E_{\mathfrak{b}} = [\mathfrak{b}] * E_0$, the advantage of a PPT solver $\mathcal{S}$ in the CSI-CDH problem is defined as*

$$\mathsf{Adv}^{\mathsf{csi\text{-}cdh}}_{G,X}(\mathcal{S}) = \Pr[\mathcal{S}(E_0, E_{\mathfrak{a}}, E_{\mathfrak{b}}) \to ([\mathfrak{a}][\mathfrak{b}]) * E_0].$$

[2] In [6], assumptions are defined as a generalized form for n-way by using cryptographic invariant maps (CIM). In the case of $n = 1$, CIM is the same as HHS.

The CSI-CDH problem corresponds to the classical computational DH problem.

Protocol of CSIDH. Here, we recall the protocol of CSIDH [11].

Public Parameters. Let $p = (4 \cdot \ell_1 \cdots \ell_{n-1})$ be a large prime where each ℓ_i is a small distinct odd prime. Then, the supersingular elliptic curve $E_0 : y^2 = x^3 + x$ over $\mathbb{F}_p$ with endomorphism ring $\mathcal{O} = \mathbb{Z}[\pi]$ is constructed where π is the Frobenius endomorphism satisfying $\pi^2 = -p$. For the notation of HHS, G is denoted by $\mathrm{cl}(\mathcal{O})$ and X is denoted by $\mathcal{ELL}_p(\mathcal{O})$; and thus, $E_0 \in X = \mathcal{ELL}_p(\mathcal{O})$. $[\mathfrak{g}] \in_R G$ means that integers $(e_1, \ldots, e_n)$ are randomly sampled from a range $\{-m, \ldots, m\}$ and $[\mathfrak{g}] = [\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}] \in \mathrm{cl}(\mathcal{O})$ where $\mathfrak{l}_i = (\ell_i, \pi - 1)$. $[\mathfrak{g}] * E_0$ is represented by the Montgomery coefficient $c \in \mathbb{F}_p$ of the elliptic curve $[\mathfrak{g}]E_0 : y^2 = x^3 + cx^2 + x$ by applying the action of $[\mathfrak{g}]$ to E_0.

The public parameters are (G, X, E_0).

Session. Parties A and B executes a key exchange session as follows:

1. Party A chooses $[\mathfrak{a}] \in_R G$, and sends the public key $\hat{A} = [\mathfrak{a}] * E_0$ to party B.
2. Party B chooses $[\mathfrak{b}] \in_R G$, and sends the public key $\hat{B} = [\mathfrak{b}] * E_0$ to party A.
3. On receiving $\hat{B}$, party A generates the session key $SK = [\mathfrak{a}] * \hat{B}$.
4. On receiving $\hat{A}$, party B generates the session key $SK = [\mathfrak{b}] * \hat{A}$.

Since G is an abelian group, $[\mathfrak{a}][\mathfrak{b}] = [\mathfrak{b}][\mathfrak{a}]$ holds. Therefore, $[\mathfrak{a}] * \hat{B} = [\mathfrak{a}] * ([\mathfrak{b}] * E_0) = ([\mathfrak{a}][\mathfrak{b}]) * E_0 = ([\mathfrak{b}][\mathfrak{a}]) * E_0 = [\mathfrak{b}] * ([\mathfrak{a}] * E_0) = [\mathfrak{b}] * \hat{A}$ holds from Definition 2.

It is obvious that the session key SK is hard to find for any passive adversary if the CSI-CDH problem is hard.

2.3 EKE

Here, we recall the protocol of EKE [3,4].

Public Parameters. Let p be a λ-bit prime, G' be a cyclic group of order p with a generator g'. Let $H : \{0,1\}^* \to \{0,1\}^\lambda$ be a hash function modelled as a RO. Let $(\mathsf{Enc}, \mathsf{Enc}^{-1})$ be a symmetric key encryption scheme with key size κ bit and input/output size ℓ-bit where $\mathsf{Enc} : \{0,1\}^\kappa \times \{0,1\}^\ell \to \{0,1\}^\ell$ is the encryption algorithm. It is modelled as an IC; that is, for each key k it is equivalent to a random permutation. Then, output a public parameter $params := (p, g', G', H, (\mathsf{Enc}, \mathsf{Enc}^{-1}))$.

Session. Parties A and B having password $pw = pw_{AB}$ executes a key exchange session as follows:

1. Party A chooses $a \in_R \mathbb{Z}_p$, computes $\hat{A} = g'^a$, and sends $\alpha = \mathsf{Enc}_{pw}(\hat{A})$ to party B.
2. Party B chooses $b \in_R \mathbb{Z}_p$, computes $\hat{B} = g'^b$, and sends $\beta = \mathsf{Enc}_{pw}(\hat{B})$ to party A.

3. On receiving β, party A decrypts $\hat{B} = \mathsf{Enc}_{pw}^{-1}(\beta)$ and generates the session key $SK = H(A, B, \hat{A}, \hat{B}, \hat{B}^a)$.
4. On receiving α, party B decrypts $\hat{A} = \mathsf{Enc}_{pw}^{-1}(\alpha)$ and generates the session key $SK = H(A, B, \hat{A}, \hat{B}, \hat{A}^b)$.

We briefly explain why the IC is necessary. In EKE, password pw is used as the key of the symmetric key encryption scheme. However, pw is chosen from dictionary $\mathcal{D}$ which is smaller than the key size. Thus, if we use a concrete symmetric key encryption scheme, security is not guaranteed in the provable way. On the other hand, in the IC model, the adversary must pose query (k, m) to Enc (or query (k, c) to Enc^{-1}) in order to do encryption (or decryption). Also, the IC is guaranteed to be independent random permutations for distinct keys. Hence, the adversary must guess the password and pose query $(pw', \cdot)$ to the IC in order to impersonate a party. Its successful probability is bounded by the number of Send query because the IC guarantees information-theoretic security.

2.4 BPR Model

Here, we recall the BPR model [3] for PAKE.

Protocol Participants and Passwords. A PAKE scheme contains two parties (an initiator and a responder, or a client and a server) who will engage in the protocol. We suppose that the total number of parties in the system is at most N. Let passwords for all pairs of parties be uniformly and independently chosen from a fixed dictionary $\mathcal{D}$. This uniformity requirement is made for simplicity and can be easily removed by adjusting security of an individual password to be the min-entropy of the distribution, instead of $1/|\mathcal{D}|$. Parties P and P' share a password $pw_{PP'}$.

Session. We denote with Π_P^i the i^{th} instance of key exchange sessions that party P runs. Each party can concurrently execute the protocol multiple times with different instances. We suppose that the total number of instances of a party is at most ℓ. The adversary is given oracle access to these instances and may also control some of the instances itself. We remark that unlike the standard notion of an "oracle", in this model instances maintain state which is updated as the protocol progresses. In particular the state of an instance Π_P^i includes the following variables (initialized as null):

- sid_P^i: the session identifier which is the ordered concatenation of all messages sent and received by Π_P^i;
- pid_P^i: the partner identifier whom Π_P^i believes it is interacting ($\mathsf{pid}_P^i \neq P$);
- acc_P^i: a Boolean variable corresponding to whether Π_P^i accepts or rejects at the end of the execution.

We say that two instances Π_P^i and $\Pi_{P'}^j$ are partnered if the following properties hold: $\mathsf{pid}_P^i = P'$ and $\mathsf{pid}_{P'}^j = P$, and $\mathsf{sid}_P^i = \mathsf{sid}_{P'}^j \neq null$ except possibly for the

final message.[3] Partnered parties must accept and conclude with the common session key.

Security Definition. An adversary is given total control of the external network connecting parties. This adversarial capability is modeled by giving some oracle accesses[4] as follows:

- $\mathsf{Execute}(P, i, P', j)$: This query models passive attacks. The output of this query consists of the messages that were exchanged during the honest execution of the protocol.
- $\mathsf{Send}(P, i, m)$: This query models active attacks. The instance Π_P^i runs according to the protocol specification and updates state. The output of this query consists of the message that the party P would generate on receipt of message m. If the input message is empty (say $\perp$), the query means activating the initiator and the output of the query consists of the first move message.
- $\mathsf{Reveal}(P, i)$: This query models leakage of session keys by improper erasure of session keys after use or compromise of a host machine. The output of this query consists of the session key SK of Π_P^i if $\mathsf{acc}_P^i = 1$.
- $\mathsf{Test}(P, i)$: At the beginning a hidden bit b is chosen. If no session key for instance Π_P^i is defined, then return the undefined symbol $\perp$. Otherwise, return the session key for instance Π_P^i if $b = 1$ or a random key from the same domain if $b = 0$. This query is posed just once.

The adversary is considered successful if it non-trivially guesses b correctly or if it breaks correctness of a session.

Definition 5 (Freshness). *We say that an instance Π_P^i is fresh unless one of the following is true at the conclusion of the experiment:*

- *the adversary poses* $\mathsf{Reveal}(P, i)$,
- *the adversary poses* $\mathsf{Reveal}(P', j)$ *if* Π_P^i *and* $\Pi_{P'}^j$ *are partnered.*

We say that an adversary $\mathcal{A}$ succeeds if either:

- $\mathcal{A}$ poses $\mathsf{Test}(P, i)$ for a fresh instance Π_P^i and outputs a bit $b' = b$,
- Π_P^i and $\Pi_{P'}^j$ are partnered, and $\mathsf{acc}_P^i = \mathsf{acc}_{P'}^i = 1$, but session keys are not identical.

The adversary's advantage for protocol Π is formally defined by:

$$\mathsf{Adv}_{\Pi,\mathcal{D}}^{\mathrm{pake}}(\mathcal{A}) = |\Pr[\mathcal{A} \text{ succeeds}] - 1/2|,$$

where λ is a security parameter.

[3] The exception of the final message for matching of sid is needed to rule out a trivial attack that an adversary forwards all messages except the final one.

[4] The model does not contain any explicit corruption oracle access (i.e., to reveal passwords). In the password-only setting, such an oracle is unnecessary because an adversary can internally simulate these oracles by itself. Please see [22, pp.190, footnote 8] for details.

Definition 6 (Security of PAKE). *We say a PAKE protocol is secure if for a dictionary $\mathcal{D}$ and any PPT adversary $\mathcal{A}$ that makes at most q_{Send} queries of* Send *to different instances the advantage* $\mathsf{Adv}^{\mathrm{pake}}_{\Pi,\mathcal{D}}(\mathcal{A})$ *is only negligibly larger than* $q_{\mathsf{Send}}/|\mathcal{D}|$ *for* λ.

3 (C)SIDH-EKE: PAKE from Isogeny Under (C)SI-CDH Assumption

In this section, we show our new PAKE schemes based on SIDH and CSIDH, named SIDH-EKE and CSIDH-EKE, respectively.

3.1 SIDH-EKE

Our first scheme (SIDH-EKE) is obtained by a combination of SIDH and EKE. SIDH-EKE relies on the RO model and the IC model as EKE. The protocol is basically the same as EKE. Though EKE is based on the classical DH key exchange, SIDH-EKE uses SIDH to share a key material between users. Specifically, each user encrypts the public key of SIDH (i.e., $\hat{A} = (E_A, \psi_A(P_B), \psi_A(Q_B))$ and $\hat{B} = (E_B, \psi_B(P_A), \psi_B(Q_A)))$ with the password as the key for the IC, decrypts the public key of the peer, and computes the session key of SIDH (i.e., $j(E/\langle R_A, R_B\rangle))$ as the key material of our scheme. In the session key generation, public keys are contained in inputs of the hash function as EKE, but j-invariants of a part of public keys are used to reduce the bandwidth.

The protocol of SIDH-EKE is as follows.

Public Parameters. Let (E, P_A, Q_A, P_B, Q_B) be the public parameters of SIDH. Let $H : \{0,1\}^* \to \{0,1\}^\lambda$ be a hash function modelled as a RO. Let $(\mathsf{Enc}, \mathsf{Enc}^{-1})$ be a symmetric key encryption scheme modelled as an IC with key size κ bit $(2^\kappa > |\mathcal{D}|)$ and domain $(\mathbb{F}_{p^2})^2 \times (\mathbb{Z}/\ell_A^{e_A}\mathbb{Z})^2$. Then, output a public parameter $params := (E, P_A, Q_A, P_B, Q_B, H, (\mathsf{Enc}, \mathsf{Enc}^{-1}))$.

Session. Parties A and B having password $pw = pw_{AB}$ executes a key exchange session as follows:

1. Party A chooses $a \in_R \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$, computes $R_A = P_A + aQ_A$, $\psi_A : E \to E_A = E/\langle R_A\rangle$ and $\hat{A} = (E_A, \psi_A(P_B), \psi_A(Q_B))$, and sends $(A, \alpha = \mathsf{Enc}_{pw}(\hat{A}))$ to party B.
2. Party B chooses $b \in_R \mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$, computes $R_B = P_B + bQ_B$, $\psi_B : E \to E_B = E/\langle R_B\rangle$ and $\hat{B} = (E_B, \psi_B(P_A), \psi_B(Q_A))$, and sends $(B, \beta = \mathsf{Enc}_{pw}(\hat{B}))$ to party A.
3. On receiving (B, β), party A decrypts $\hat{B} = \mathsf{Enc}^{-1}_{pw}(\beta)$, computes $R_{BA} = \psi_B(P_A) + a\psi_B(Q_A)$ and $Z = j(E_B/\langle R_{BA}\rangle)$, and generates the session key $SK = H(A, B, j(E_A), j(E_B), Z)$.
4. On receiving (A, α), party B decrypts $\hat{A} = \mathsf{Enc}^{-1}_{pw}(\alpha)$, computes $R_{AB} = \psi_A(P_B) + b\psi_A(Q_B)$ and $Z = j(E_A/\langle R_{AB}\rangle)$, and generates the session key $SK = H(A, B, j(E_A), j(E_B), Z)$.

Security. Here, we show security of SIDH-EKE in the BPR model. The security proof is slightly different with the security proof of EKE due to the structure of the SIDH system. In EKE, if we set $\hat{A} = g^a \cdot g^\theta$ and $\hat{B} = g^b \cdot g^\phi$, the session key is $SK = H(A, B, \hat{A}, \hat{B}, Z = g^{ab} \cdot g^{a\phi} \cdot g^{b\theta} \cdot g^{\theta\phi})$. Thus, in the EKE proof, in order to change the session key generation in the $\mathsf{Execute}$ oracle, the simulator embeds instances of the CDH problem to g^a and g^b, sets public keys as above by choosing θ and ϕ for each session, and finally obtains g^{ab} (i.e., the answer of the CDH problem) from Z. However, in SIDH-EKE, such a simulation does not work because $j(E_A)$ and $j(E_B)$ have no algebraic structure (i.e., j-invariants). Specifically, for $j(E_A)\cdot j(E_\theta)$ and $j(E_B)\cdot j(E_\phi)$, $Z = j(E_A/\langle R_{AB}\rangle)\cdot j(E_A/\langle R_{A\phi}\rangle)\cdot j(E_B/\langle R_{B\theta}\rangle) \cdot j(E_\theta/\langle R_{\theta\phi}\rangle)$ is not guaranteed. Hence, in our proof, we simulate the $\mathsf{Execute}$ oracle gradually by using the hybrid argument. Specifically, the output of the $\mathsf{Execute}$ query is gradually changed in hybrid experiments, and the simulator sets the public keys of the changed session to be the same as instances of the SI-CDH problem. The simulator directly obtains the answer of the SI-CDH problem as Z for each hybrid experiment. Also, our scheme is secure against off-line dictionary attacks. E_A in the ephemeral public key $\hat{A}$ is an elliptic curve having form $y^2 = x^3 + \alpha x^2 + \beta$ for $\alpha, \beta \in \mathbb{F}_{p^2}$, and $\psi_A(P_B), \psi_A(Q_B) \in \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$ are some points of E_A. Hence, $\mathsf{Enc}_{pw}(\hat{A})$ is the ciphertext of $(\alpha, \beta, \psi_A(P_B), \psi_A(Q_B))$. The adversary can observe $\mathsf{Enc}_{pw}(\hat{A})$ and try to find pw by posing $(pw', \mathsf{Enc}_{pw}(\hat{A}))$ to Enc^{-1} oracle for guessing password pw'. However, since any information of $(\alpha, \beta, \psi_A(P_B), \psi_A(Q_B))$ is not leaked from $\mathsf{Enc}_{pw}(\hat{A})$ because $(\mathsf{Enc}, \mathsf{Enc}^{-1})$ is the IC, the adversary cannot determine if the guess is valid or not. Thus, our scheme prevents off-line dictionary attacks. Therefore, we can prove security of SIDH-EKE.

Theorem 1. *For the advantage* $\mathsf{Adv}^{\mathsf{si\text{-}cdh}}_{E,\ell_A,\ell_B}(\mathcal{S})$ *of the SI-CDH problem, the advantage* $\mathsf{Adv}^{\mathrm{pake}}_{\mathsf{sidh\text{-}eke},\mathcal{D}}(\mathcal{A})$ *of CSIDH-EKE is as follows in the RO model and the IC model:*

$$\mathsf{Adv}^{\mathrm{pake}}_{\mathsf{sidh\text{-}eke},\mathcal{D}}(\mathcal{A}) \leq \frac{(q_{\mathsf{Send}} + q_{\mathsf{Execute}})^2}{4p^2} + (q_{\mathsf{Execute}} + q_{\mathsf{Send}}) \cdot \mathsf{Adv}^{\mathsf{si\text{-}cdh}}_{E,\ell_A,\ell_B}(\mathcal{S}) + \frac{q_{\mathsf{Send}}}{|\mathcal{D}|}$$

where q_{Send} *and* q_{Execute} *denote the upper bound of* Send *and* $\mathsf{Execute}$ *queries, respectively.*

3.2 CSIDH-EKE

Our second scheme (CSIDH-EKE) is obtained by a combination of CSIDH and EKE as SIDH-EKE. Specifically, each user encrypts the public key of CSIDH (i.e., $\hat{A}$ or $\hat{B}$) with the password as the key for the IC, decrypts the public key of the peer, and computes the session key of CSIDH (i.e., $([\mathfrak{a}][\mathfrak{b}]) * E_0$) as the key material of our scheme.

The protocol of CSIDH-EKE is as follows.

Public Parameters. Let (G, X) be an abelian group and a finite set constructing HHS, and $E_0 \in X$ be the supersingular elliptic curve $E_0 : y^2 = x^3 + x$ over $\mathbb{F}_p$. Let $H : \{0,1\}^* \to \{0,1\}^\lambda$ be a hash function modelled as a RO. Let $(\mathsf{Enc}, \mathsf{Enc}^{-1})$ be a symmetric key encryption scheme modelled as an IC with key size κ bit ($2^\kappa > |\mathcal{D}|$) and domain $\mathbb{F}_p$. Then, output a public parameter $params := (G, X, E_0, H, (\mathsf{Enc}, \mathsf{Enc}^{-1}))$.

Session. Parties A and B having password $pw = pw_{AB}$ executes a key exchange session as follows:

1. Party A chooses $[\mathfrak{a}] \in_R G$, computes $\hat{A} = [\mathfrak{a}] * E_0$, and sends $(A, \alpha = \mathsf{Enc}_{pw}(\hat{A}))$ to party B.
2. Party B chooses $[\mathfrak{b}] \in_R G$, computes $\hat{B} = [\mathfrak{b}] * E_0$, and sends $(B, \beta = \mathsf{Enc}_{pw}(\hat{B}))$ to party A.
3. On receiving (B, β), party A decrypts $\hat{B} = \mathsf{Enc}^{-1}_{pw}(\beta)$ and generates the session key $SK = H(A, B, \hat{A}, \hat{B}, [\mathfrak{a}] * \hat{B})$.
4. On receiving (A, α), party B decrypts $\hat{A} = \mathsf{Enc}^{-1}_{pw}(\alpha)$ and generates the session key $SK = H(A, B, \hat{A}, \hat{B}, [\mathfrak{b}] * \hat{B})$.

Security. Security of CSIDH-EKE can be proved by a similar manner as SIDH-EKE. Here, we discuss security against off-line dictionary attacks. $\hat{A}$ corresponds to the Montgomery coefficient $c \in \mathbb{F}_p$ of the elliptic curve $[\mathfrak{a}]E_0 : y^2 = x^3 + cx^2 + x$ by applying the action of $[\mathfrak{a}]$ to E_0. Hence, $\mathsf{Enc}_{pw}(\hat{A})$ is the ciphertext of c. The adversary can observe $\mathsf{Enc}_{pw}(\hat{A})$ and try to find pw by posing $(pw', \mathsf{Enc}_{pw}(\hat{A}))$ to Enc^{-1} oracle for guessing password pw'. However, since any information of c is not leaked from $\mathsf{Enc}_{pw}(\hat{A})$ because $(\mathsf{Enc}, \mathsf{Enc}^{-1})$ is the IC, the adversary cannot determine if the guess is valid or not. Thus, CSIDH-EKE prevents off-line dictionary attacks.

Theorem 2. *For the advantage* $\mathsf{Adv}^{\mathsf{csi\text{-}cdh}}_{G,X}$ *of the CSI-CDH problem, the advantage* $\mathsf{Adv}^{\mathrm{pake}}_{\mathsf{csidh\text{-}eke},\mathcal{D}}$ *of CSIDH-EKE is as follows in the RO model and the IC model:*

$$\mathsf{Adv}^{\mathrm{pake}}_{\mathsf{csidh\text{-}eke},\mathcal{D}}(\mathcal{A}) \leq \frac{(q_{\mathsf{Send}} + q_{\mathsf{Execute}})^2}{2p} + (q_{\mathsf{Execute}} + q_{\mathsf{Send}}) \cdot \mathsf{Adv}^{\mathsf{csi\text{-}cdh}}_{G,X}(\mathcal{S}) + \frac{q_{\mathsf{Send}}}{|\mathcal{D}|}$$

where q_{Send} *and* q_{Execute} *denote the upper bound of* Send *and* Execute *queries, respectively.*

4 Comparison

In this section, we give an efficiency comparison of our schemes and the TSJL scheme [38]. The comparison is shown in Table 1.

Table 1. Comparison among PAKE from isogeny

	Assumption	Communication overhead	Computational time
TJSL scheme [38]	SI-CDH & SI-APC & SI-APD & C-SGA	2640 bit	≈ 5.0 ms
SIDH-EKE (Sect. 3.1)	SI-CDH	2640 bit	≈ 5.0 ms
CSIDH-EKE (Sect. 3.2)	CSI-CDH	512 bit	≈ 80.6 ms

SI-APC, SI-APD and C-SGA mean the supersingular isogeny auxiliary point computation assumption, the supersingular isogeny auxiliary point decision assumption and the computational simultaneous group action assumption, respectively, introduced in [38].

To compare SIDH-based schemes and the CSIDH-based scheme, we use parameters having the same security level (i.e., NIST category 1 [1]) corresponding to the key search on a block cipher with a 128 bit key (i.e., $\kappa = 128$). For SIDH, the parameter corresponding to NIST category 1 is estimated as SIKE$p434$ in [24]. The public key is an element in $(\mathbb{F}_{p^2})^2 \times (\mathbb{Z}/\ell_A^{e_A}\mathbb{Z})^2$, and the size is estimated as 2640 bit. Computational time of a public key generation and time for a session key generation of SIDH are about 1.9 ms and about 3.1 ms, respectively, based on the performance evaluation of x64-assembly implementation on a 3.4GHz Intel Core i7-6700 (Skylake) processor in [24, Table 2.1]. The TSJL scheme and SIDH-EKE contain an ephemeral public key of SIDH as the message, and computations of a public key generation and a session key generation of SIDH for each party. For CSIDH, the parameter corresponding to NIST category 1 is estimated as CSIDH-512 in [11]. The public key is an element in $\mathbb{F}_p$, and the size is estimated as 512 bit. Computational time of a group action and time for a public key validation of CSIDH are about 40.3 ms and about 1.6 ms, respectively, based on the proof-of-concept implementation on a 3.5GHz Intel Core i5 (Skylake) processor in [11, Table 2]. CSIDH-EKE contains an ephemeral public key of CSIDH as the message, and computations of a public key generation and a session key generation of CSIDH for each party. We simply add these values without any acceleration technique. As shown in Table 1, CSIDH-EKE is more compact than the TSJL scheme, and SIDH-EKE is secure only under the SI-CDH assumption while the TSJL scheme relies on additional assumptions.

5 Conclusion

We introduced two new one-round PAKE schemes, SIDH-EKE and CSIDH-EKE, based on isogeny, which are secure under the standard hardness assumptions. Also, CSIDH-EKE is advantageous in communication overhead though the computational cost is worse. The security proof follows the proof of EKE in the RO and IC model, but there is a technical issue due to the difference between algebraic structures of EKE and (C)SIDH-EKE. Excluding symmetric cryptography operations, the computational cost and communication cost of (C)SIDH-EKE is almost the same as original (C)SIDH.

A remaining problem of further researches is removing idealized building blocks such as ROs and ICs. Otherwise, giving a security proof in the quantum RO (or IC) model is another direction.

References

1. Post-Quantum Cryptography Standardization. National Institute of Standards and Technology (2016)
2. Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: Post-quantum key exchange - a new hope. In: USENIX Security Symposium 2016, pp. 327–343 (2016)
3. Bellare, M., Pointcheval, D., Rogaway, P.: Authenticated key exchange secure against dictionary attacks. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 139–155. Springer, Heidelberg (2000). https://doi.org/10.1007/3-540-45539-6_11
4. Bellovin, S.M., Merritt, M.: Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password file compromise. In: ACM CCS, pp. 244–250 (1993)
5. Ben Hamouda, F., Blazy, O., Chevalier, C., Pointcheval, D., Vergnaud, D.: Efficient UC-secure authenticated key-exchange for algebraic languages. In: Kurosawa, K., Hanaoka, G. (eds.) PKC 2013. LNCS, vol. 7778, pp. 272–291. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-36362-7_18
6. Boneh, D., et al.: Multiparty non-interactive key exchange and more from isogenies on elliptic curves. In: MATHCRYPT 2018 (2018). https://eprint.iacr.org/2018/665
7. Bos, J.W., et al.: Frodo: take off the ring! Practical, quantum-secure key exchange from LWE. In: ACM Conference on Computer and Communications Security 2016, pp. 1006–1018 (2016)
8. Bos, J.W., Costello, C., Naehrig, M., Stebila, D.: Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. In: IEEE Symposium on Security and Privacy 2015, pp. 553–570 (2015)
9. Boyko, V., MacKenzie, P.D., Patel, S.: Provably secure password-authenticated key exchange using Diffie-Hellman. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 156–171. Springer, Heidelberg (2000). https://doi.org/10.1007/3-540-45539-6_12
10. Canetti, R., Dachman-Soled, D., Vaikuntanathan, V., Wee, H.: Efficient password authenticated key exchange via oblivious transfer. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 449–466. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-30057-8_27
11. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: an efficient post-quantum commutative group action. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018. LNCS, vol. 11274, pp. 395–427. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-03332-3_15
12. Childs, A.M., Jao, D., Soukharev, V.: Constructing elliptic curve isogenies in quantum subexponential time. J. Math. Cryptol. **8**(1), 1–29 (2014)
13. Couveignes, J.M.: Hard Homogeneous Spaces. Cryptology ePrint Archive, Report 2006/291 (2006). https://eprint.iacr.org/2006/291
14. Ding, J., Alsayigh, S., Lancrenon, J., RV, S., Snook, M.: Provably secure password authenticated key exchange based on RLWE for the post-quantum world. In: Handschuh, H. (ed.) CT-RSA 2017. LNCS, vol. 10159, pp. 183–204. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-52153-4_11

15. Ding, J., Xie, X., Lin, X.: A simple provably secure key exchange scheme based on the learning with errors problem. IACR Cryptology ePrint Archive 2012/688 (2012). http://eprint.iacr.org/2012/688
16. Feo, L.D., Jao, D., Plût, J.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. J. Math. Cryptol. **8**(3), 209–247 (2014)
17. Fujioka, A., Suzuki, K., Xagawa, K., Yoneyama, K.: Strongly secure authenticated key exchange from factoring, codes, and lattices. Des. Codes Crypt. **76**(3), 469–504 (2015)
18. Fujioka, A., Takashima, K., Terada, S., Yoneyama, K.: Supersingular isogeny Diffie–Hellman authenticated key exchange. In: Lee, K. (ed.) ICISC 2018. LNCS, vol. 11396, pp. 177–195. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-12146-4_12
19. Galbraith, S.D.: Authenticated key exchange for SIDH. IACR Cryptology ePrint Archive 2018/266 2018 (2018). http://eprint.iacr.org/2018/266
20. Gennaro, R.: Faster and shorter password-authenticated key exchange. In: Canetti, R. (ed.) TCC 2008. LNCS, vol. 4948, pp. 589–606. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-78524-8_32
21. Gennaro, R., Lindell, Y.: A framework for password-based authenticated key exchange. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 524–543. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-39200-9_33
22. Gennaro, R., Lindell, Y.: A framework for password-based authenticated key exchange. ACM Trans. Inf. Syst. Secur. **9**(2), 181–234 (2006)
23. Groce, A., Katz, J.: A new framework for efficient password-based authenticated key exchange. In: ACM Conference on Computer and Communications Security 2010, pp. 516–525 (2010)
24. Jao, D., et al.: Supersingular Isogeny Key Encapsulation (SIKE). submission to NIST PQC Competition (2017). https://sike.org/
25. Jao, D., De Feo, L.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: Yang, B.-Y. (ed.) PQCrypto 2011. LNCS, vol. 7071, pp. 19–34. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25405-5_2
26. Jiang, S., Gong, G.: Password based key exchange with mutual authentication. In: Handschuh, H., Hasan, M.A. (eds.) SAC 2004. LNCS, vol. 3357, pp. 267–279. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-30564-4_19
27. Jutla, C., Roy, A.: Relatively-sound NIZKs and password-based key-exchange. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 485–503. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-30057-8_29
28. Katz, J., Ostrovsky, R., Yung, M.: Efficient password-authenticated key exchange using human-memorable passwords. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 475–494. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44987-6_29
29. Katz, J., Ostrovsky, R., Yung, M.: Forward secrecy in password-only key exchange protocols. In: Cimato, S., Persiano, G., Galdi, C. (eds.) SCN 2002. LNCS, vol. 2576, pp. 29–44. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-36413-7_3
30. Katz, J., Ostrovsky, R., Yung, M.: Efficient and secure authenticated key exchange using weak passwords. J. ACM **57**(1), 1–39 (2009)
31. Katz, J., Vaikuntanathan, V.: Smooth projective hashing and password-based authenticated key exchange from lattices. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 636–652. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-10366-7_37

32. Katz, J., Vaikuntanathan, V.: Round-optimal password-based authenticated key exchange. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 293–310. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19571-6_18
33. LeGrow, J., Jao, D., Azarderakhsh, R.: Modeling Quantum-Safe Authenticated Key Establishment, and an Isogeny-Based Protocol. IACR Cryptology ePrint Archive 2018/282 (2018). http://eprint.iacr.org/2018/282
34. Longa, P.: A Note on Post-Quantum Authenticated Key Exchange from Supersingular Isogenies. IACR Cryptology ePrint Archive 2018/267 (2018). http://eprint.iacr.org/2018/267
35. MacKenzie, P., Patel, S., Swaminathan, R.: Password-authenticated key exchange based on RSA. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 599–613. Springer, Heidelberg (2000). https://doi.org/10.1007/3-540-44448-3_46
36. Peikert, C.: He Gives C-Sieves on the CSIDH. Cryptology ePrint Archive, Report 2019/725 (2019). https://eprint.iacr.org/2006/291
37. Rostovtsev, A., Stolbunov, A.: Public-Key Cryptosystem Based on Isogenies. Cryptology ePrint Archive, Report 2006/145 (2006). https://eprint.iacr.org/2006/145
38. Taraskin, O., Soukharev, V., Jao, D., LeGrow, J.: An Isogeny-Based Password-Authenticated Key Establishment Protocol. IACR Cryptology ePrint Archive 2018/886 (2018). https://eprint.iacr.org/2018/886
39. Vélu, J.: Isogénies entre courbes elliptiques. Comptes Rendus des Séances de l'Académie des Sciences. Série I. Mathématique **273**, A238–A241 (1971)
40. Xu, X., Xue, H., Wang, K., Tian, S., Liang, B., Yu, W.: Strongly Secure Authenticated Key Exchange from Supersingular Isogeny. IACR Cryptology ePrint Archive 2018/760 (2018)