

# Strongly Secure Authenticated Key Exchange from Supersingular Isogenies

Xiu Xu<sup>1,2,4</sup>, Haiyang Xue<sup>1,2,3</sup> ✉, Kunpeng Wang<sup>1,2,4</sup>, Man Ho Au<sup>3</sup>, Song  
Tian<sup>1,2</sup>

<sup>1</sup> State Key Laboratory of Information Security, Institute of Information Engineering,  
Chinese Academy of Sciences, Beijing, China

<sup>2</sup> Data Assurance and Communications Security Research Center, Beijing, China

<sup>3</sup> The Hong Kong Polytechnic University, Hong Kong

<sup>4</sup> School of Cyber Security, University of Chinese Academy of Sciences, China.  
haiyangxc@gmail.com

**Abstract.** This paper aims to address the open problem, namely, to find new techniques to design and prove security of supersingular isogeny-based authenticated key exchange (AKE) protocols against the widest possible adversarial attacks, raised by Galbraith in 2018. Concretely, we present two AKEs based on a double-key PKE in the supersingular isogeny setting secure in the sense of  $\text{CK}^+$ , one of the strongest security models for AKE. Our contributions are summarised as follows. Firstly, we propose a strong OW-CPA secure PKE,  $2\text{PKE}_{\text{sidh}}$ , based on SI-DDH assumption. By applying modified Fujisaki-Okamoto transformation, we obtain a [OW-CCA, OW-CPA] secure KEM,  $2\text{KEM}_{\text{sidh}}$ . Secondly, we propose a two-pass AKE,  $\text{SIAKE}_2$ , based on SI-DDH assumption, using  $2\text{KEM}_{\text{sidh}}$  as a building block. Thirdly, we present a modified version of  $2\text{KEM}_{\text{sidh}}$  that is secure against leakage under the 1-Oracle SI-DH assumption. Using the modified  $2\text{KEM}_{\text{sidh}}$  as a building block, we then propose a three-pass AKE,  $\text{SIAKE}_3$ , based on 1-Oracle SI-DH assumption. Finally, we prove that both  $\text{SIAKE}_2$  and  $\text{SIAKE}_3$  are  $\text{CK}^+$  secure in the random oracle model and supports arbitrary registration. We also provide an implementation to illustrate the efficiency of our schemes. Our schemes compare favourably against existing isogeny-based AKEs. To the best of our knowledge, they are the first of its kind to offer security against arbitrary registration, wPFS, KCI, and MEX simultaneously. Regarding efficiency, our schemes outperform existing schemes in terms of bandwidth as well as CPU cycle count.

**Keywords:** authenticated key exchange, key encapsulation mechanism, supersingular elliptic curve isogeny, post quantum

## 1 Introduction

**Authenticated Key Exchange.** Allowing two parties to agree on a common shared key over a public but possibly insecure channel, key exchange (KE) is a fundamental cryptographic primitive. Many studies have investigated how to

achieve KE protocols that provide authentication [4,6,12,27] and how to implement authenticated key exchange (AKE) with high efficiency [2,12,13,21,27,28,29] based on classical assumptions. Different of security models have been proposed, including BR model [4], CK model [6] and eCK model [27]. Introduced in [22] and reformulated by Fujioka et al. [12], currently,  $CK^+$  security model is known as one of the ‘strongest’ and most ‘desirable’ security notions. The  $CK^+$  model not only covers the security requirement in CK model, but also captures some advanced attacks such as the key compromise impersonation (KCI) attack, the maximal exposure (MEX) attack and the breaking of weak perfect forward secrecy (wPFS).

**Supersingular Isogeny Diffie-Hellman Key Exchange (SIDH).** Apart from lattice, code, hash and multivariate cryptography, supersingular elliptic curve isogeny is one of the most attractive candidates for post-quantum cryptography. The best-known protocol is Jao and De Feo’s supersingular isogeny Diffie-Hellman key exchange (SIDH) [8] based on the hard problem of computing isogenies between supersingular elliptic curves. There are several interesting topics concerning SIDH in the literature. For example, computational efficiency [7,10,23], key compression [5], adaptive attacks on SIDH [17], relationship of the underlying complexity problems [9,19,32], signature schemes [16,31,35] and its standardization [20,24].

Recently, several work [14,15,26] have studied the important problem of designing AKE schemes from the basic SIDH primitive. As pointed out by Galbraith [15], there are several challenges in adapting the security proof of existing well-designed AKE schemes (most of them are based on discrete logarithm assumption) to the SIDH case:

- Many AKE schemes based on discrete logarithm assumption, such as MQV [28] and HMQV [22], require a richer algebraic structure the supersingular isogeny does not possess.
- The protocols involving long-term/static secret keys are vulnerable to the adaptive attack [17] aiming at the case where the static public key is used. More precisely, suppose that in a protocol Alice sets  $E_A$  as her static public key, and  $E_Y$  is an ephemeral public value sent by Bob. Galbraith et al. [17] showed that adversary Bob can send  $(E_Y, R', S')$  with maliciously-crafted points  $R'$  and  $S'$  to gradually learn Alice’s static secret key.
- The gap assumption that holds in the discrete logarithm setting is crucial for security proof. However, the gap assumption does not hold in the SIDH setting when polynomial queries are submitted to an *unlimited* decisional solver.

**The State of the Art of SIDH AKE.** Recently, there are many exciting results on the generic and non-generic constructions of AKE over supersingular curves [14,15,26]. Galbraith [15] and Longa [26] showed how to adapt the generic constructions of secure AKE from basic primitives like IND-CCA encryption/KEMs, MACs, PRFs etc, including the schemes proposed by Boyd,

Cliff, Nieto and Paterson [2] (abbreviated as BCNP scheme), by Fujioka, Suzuki, Xagawa and Yoneyama [13] (abbreviated as FSXY scheme) and by Guilhem, Smart and Warinschi [18] (abbreviated as GSW scheme), to the SIDH setting by inserting an IND-CCA secure KEM based on SIDH. Particularly, Longa [26] showed how to use SIDH as basic building blocks to construct AKE schemes. However, these transformations lead either to more isogeny computations or increase in rounds of communication. The detailed analyses are examined and summarized in Table 1 of [15]. Here we make a more concrete comparison among these AKE schemes in the SIDH setting in Table 1.

With respect to non-generic constructions, Galbraith proposed two SIDH-AKE protocols [15], one of which is based on the Jeong-Katz-Lee [21] scheme TS2 (we call it Gal 1) and another is an SIDH variant of NAXOS scheme (we call it Gal 2). Very recently, Fujioka et al. [14] gave two Diffie-Hellman like isogeny-based AKEs, which we denote as FTTY 1 where the session key is extracted from the combination of two Diffie-Hellman values, and FTTY 2 where the session key is extracted from four Diffie-Hellman values, respectively. Unfortunately, all of these schemes only provide security against adversaries with limited capabilities, such as wPFS security (details are given in section 1.3). Several known attacks are not taken into account, including arbitrary registrant for static public keys, the KCI attack, or the MEX attack. In an AKE system, the adversary-controlled parties may register arbitrary public keys and arbitrary registrant allows any party to register arbitrary public keys (even the same key with some other party) without any validity checks. In fact, neither Gal 1-2 nor FTTY 1-2 scheme allows the arbitrary registrant for the static public key. Otherwise, with malicious static public keys, a target secret key can be learned bit by bit, which implies that Gal 1-2 and FTTY 1-2 are not resistant to the adaptive attack. Moreover, Gal 1 is not resistant to the KCI attack and Gal 2 is not resistant to the MEX attack. Detailed analyses on those attacks against Gal 1-2 and FTTY 1-2 are given in the related works.

Thus, “*to find new techniques to design and prove security of AKE protocols in the SIDH setting, ... give a full analysis of AKE that includes the widest possible adversarial goals.*”, a quote from Galbraith [15], is the main problem to be addressed in the area of SIDH-based AKE. In this paper, we are motivated to address such an open problem.

## 1.1 Our Contributions

In this paper, we present two AKEs based on a double-key PKE in the SIDH setting and show that both of them allow arbitrary registrant and are  $\text{CK}^+$  secure in the random oracle model. Our results are summarized as follows.

- We propose a strong OW-CPA secure PKE,  $2\text{PKE}_{\text{sidh}}$ , based on SI-DDH assumption. The strong OW-CPA security is exactly the  $[\text{OW-CPA}, \cdot]$  security formalized in [34] which states that the PKE is still OW-CPA secure even if part of the public key is generated by the adversary. This construction may

be of independent interest. Through the modified Fujisaki-Okamoto transformation [34], we obtain a [OW-CCA, OW-CPA] secure KEM,  $2\text{KEM}_{\text{sidh}}$ , to be used as the building block of our AKE.

- With  $2\text{KEM}_{\text{sidh}}$  as the basic tool, we propose a two-pass AKE,  $\text{SIAKE}_2$ , based on SI-DDH assumption.  $\text{SIAKE}_2$  is  $\text{CK}^+$  secure in the random oracle model and supports arbitrary registration.
- We propose 1-Oracle SI-DH assumption, a strong version of the SI-DDH assumption. Contrary to its analogue, Oracle Diffie-Hellman problem [1] in the discrete logarithm setting, the 1-Oracle SI-DH problem only allows one query to the oracle. We revisit  $2\text{PKE}_{\text{sidh}}$  and provide a modified version of  $2\text{KEM}_{\text{sidh}}$ , and show that under the 1-Oracle SI-DH assumption both of them are still secure against leakage.
- Using the modified  $2\text{KEM}_{\text{sidh}}$  as the basic tool, we propose a three-pass AKE,  $\text{SIAKE}_3$ , based on 1-Oracle SI-DH assumption. We prove that it supports arbitrary registration and is also  $\text{CK}^+$  secure in the random oracle model.

From Table 1, we can observe that both  $\text{SIAKE}_2$  and  $\text{SIAKE}_3$  achieve the security against multiple possible adversaries, which to the best of our knowledge covers the most extensive adversarial goals, including arbitrary registrant, wPFS, KCI and MEX.

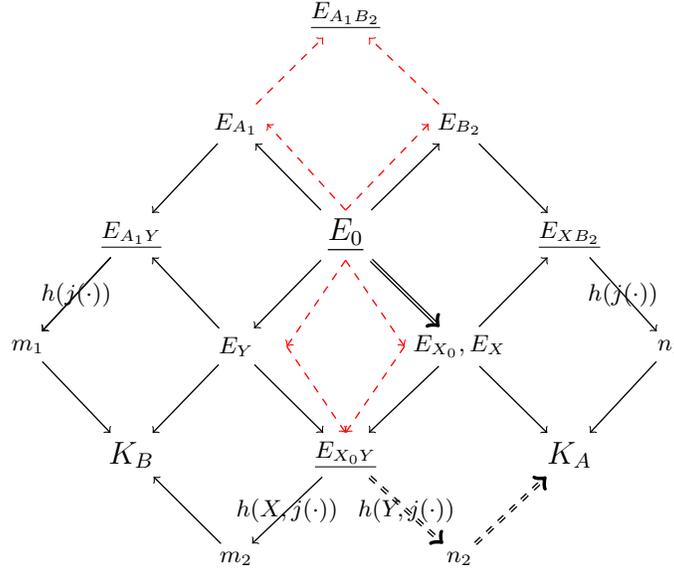
Scheme	Key Reg.	Assump.	Model	wPFS	KCI	MEX	Rd	Init isog	Resp isog	Mess Size
Gal 1 [15]	Honest	SI-CDH	CK	✓	×	×	2	3	3	$108n$
Gal 2 [15]	Honest	SI-CDH	BR	✓	✓	×	2	4	4	$108n$
FTTY 1 [14]	Honest	SI-DDH	CK	✓	×	×	1	3	3	$72n$
FTTY 2 [14]	Honest	di-SI-DDH	$\text{CK}^+$	✓	✓	✓	1	5	5	$72n$
GSW [18]	Arbi.	SI-DDH	CK	✓	×	×	3	6	6	$186n$
BCNP [2,26]	Arbi.	SI-DDH	CK	✓	✓	×	2	6	6	$148n$
FSXY [13,26]	Arbi.	SI-DDH	$\text{CK}^+$	✓	✓	✓	2	6	6	$148n$
$\text{SIAKE}_2$	Arbi.	SI-DDH	$\text{CK}^+$	✓	✓	✓	2	6	5	$114n$
$\text{SIAKE}_3$	Arbi.	1-OSIDH	$\text{CK}^+$	✓	✓	✓	3	5	5	$80n$

**Table 1.** Comparison of existing AKE protocols on supersingular isogeny. **Key Reg.** represents registering the static public key. “Arbi” means arbitrary registrant is allowed while “Honest” means only honest registrants is allowed. **Assump.** is the abbreviation of assumptions. “1-OSIDH” is the abbreviation of 1-Oracle SI-DH assumption. **Rd** denotes the number of protocol’s communication round. **Init isog** and **Resp isog** represent the number of isogeny computation that the initiator and responder have to perform respectively. **Mess Size** denotes the total message size. “✓” indicates that the scheme can resist this kind of attack while “×” indicates it cannot.  $n$  is the security parameter.

## 1.2 Technique Overview

Our core ideas and techniques are illustrated in Figure 1. Let  $E_0$  be the starting curve, and  $(P_1, Q_1), (P_2, Q_2)$  be the base points.  $E_{A_1}, E_{B_2}, E_X$  and  $E_Y$  are four intermediate curves which are part of static or ephemeral public keys.  $E_{A_1Y}, E_{XB_2}$  and  $E_{XY}$  are three final computing curves.

Let  $U_A, U_B$  be two parties in the AKEs. The SIDH works as follows:  $U_A$  chooses a secret, computes the isogeny  $\phi_X : E_0 \rightarrow E_X$  with kernel  $G_X$  and publishes  $X = (E_X, \phi_X(P_2), \phi_X(Q_2))$ .  $U_B$  chooses a secret, computes the isogeny  $\phi_Y : E_0 \rightarrow E_Y$  with kernel  $G_Y$  and publishes  $Y = (E_Y, \phi_Y(P_1), \phi_Y(Q_1))$ . They both can compute  $E_{XY} \cong E_X/\phi_X(G_Y) \cong E_Y/\phi_Y(G_X)$ . The strategy to provide authentication with the static and ephemeral components is that every user registers a static public key such that  $U_A$ 's static public key is  $pk_{A_1} = (E_{A_1}, \phi_{A_1}(P_2), \phi_{A_1}(Q_2))$  while  $U_B$ 's static public key is  $pk_{B_2} = (E_{B_2}, \phi_{B_2}(P_1), \phi_{B_2}(Q_1))$ .



**Fig. 1.** Illustration of the core idea of  $\text{SIKE}_2$  and  $\text{SIKE}_3$ . The red dashed lines illustrate the core ideas of Gal 1 scheme [15]. In  $\text{SIKE}_2$ ,  $E_X$  and  $E_{X_0}$  are two independent curves. In  $\text{SIKE}_3$ ,  $E_X = E_{X_0}$  and the dashed double arrow is included.

As shown in Figure 1, there is a natural way to extract a session key from four Diffie-Hellman values  $E_{A_1B_2}, E_{A_1Y}, E_{XB_2}$  and  $E_{XY}$  (Actually, this is what FTTY2 scheme does). However, it is risky to take  $E_{A_1B_2}$  into account. Let us recall the adaptive attack from Galbraith, Petit, Shani and Ti [17]. A malicious user  $U_B$  who registers his static public key  $E_{B_2}$  with specified points  $R', S'$ , can learn one bit of the static secret key of  $U_A$  if he can also query the session key.

As shown in Figure 1 with dashed lines, Galbraith [15] involves  $E_{A_1B_2}$  and  $E_{XY}$  for the session key. Under the adaptive attack [17], adversary could gradually learn the static secret key by malicious registrations. Thus,  $E_{A_1B_2}$  could not be included in the session key when arbitrary registrant is allowed.

Although now only  $E_{A_1Y}$ ,  $E_{XB_2}$ , and  $E_{XY}$  are involved in the session key, the adaptive attack can still be launched if the  $CK^+$  adversary (in case  $E_2$  in Table 2) sends  $E_Y$  with specified points  $R', S'$  to  $U_A$ . With the ephemeral secret key for  $E_X$  and the session key, the adversary could still extract one bit of the static secret key. The problem can be tackled by a check of “validity” of  $Y = (E_Y, R, S)$ . Our solution is to employ the “re-encryption” technique used in Fujisaki-Okamoto (FO) transformation [11]. Precisely,  $C = (Y, y_1, y_0)$  is the ciphertext under public key  $pk_{A_1}$  and  $X$ , where  $Y = (E_0 / \langle P_2 + [y]Q_2 \rangle, \phi_Y(P_1), \phi_Y(Q_1))$ ,  $y_1 = h(j(E_{A_1Y})) \oplus m_1$ ,  $y_0 = h(j(E_{XY})) \oplus m_0$  and  $y = G(m_1, m_0)$  for a hash function  $G$ , and the encapsulated key is  $K_B = H(m_1, m_0, C)$ . As a byproduct, we obtain the chosen ciphertext (CCA) secure KEM by the FO transformation and the “validity” of  $Y = (E_Y, R, S)$  can be checked by  $U_A$  using  $y = G(m_1, m_0)$  so that the adaptive attack fails to work.

Now the CCA secure KEM with “re-encryption” avoids the adaptive attack, but it is still not sufficient for  $CK^+$  security. The  $CK^+$  adversary has the capability to adaptively *send* messages and adaptively query the *session state* and *session key* of non-test sessions. The capability of adaptively *sending* messages in the test session means that the adversary is allowed to choose one-part of the challenge public key  $X^*$  for  $(Y^*, y_1^*, y_0^*)$ , while the capability of querying the *session state* and *session key* of non-test sessions implies that the adversary is also allowed to query the decapsulation oracle which decapsulates the ciphertext under several other public keys  $X'$ . This feature has been analyzed by [34] and formalized as [OW-CCA,  $\cdot$ ] security. The modified Fujisaki-Okamoto [34] states that putting the public key in the hashing step when generating the encapsulated key would be sufficient. Precisely,  $K_B$  encapsulated in  $(Y, y_1, y_0)$  is  $H(X, m_1, m_2, C)$ .

The last challenge that we are facing is the relationship between  $X$  and  $Y$ , which leads to the difficulty in simulating the  $CK^+$  game. In the test session, on the one hand  $X$  is part of the public key  $(pk_{A_1}, X)$  under which the ciphertext  $(Y, y_1, y_0)$  is computed. On the other hand  $X$  is part of the ciphertext  $(X, x_1, x_0)$  in which  $K_A$  is encapsulated under public key  $(pk_{B_2}, Y)$ . Precisely, in the test session  $X = ((E_X, R_2, S_2), x_1, x_0)$  is sent by AKE adversary  $\mathcal{A}$ , and the simulator  $\mathcal{S}$  obtains challenge ciphertext  $(Y^*, y_1^*, y_0^*)$  from the [OW-CCA,  $\cdot$ ] challenger (which means the secret  $y$  in  $Y^*$  is unknown). But to simulate the  $CK^+$  game, especially to maintain the consistency of hash lists,  $\mathcal{S}$  should learn  $h(j(E_X / \langle R_2 + [y]S_2 \rangle))$  to extract  $K_A$  encapsulated in  $(X, x_1, x_0)$ .

We propose two solutions for this problem. One method is to add an extra  $X_0$  such that  $X_0$  is part of the public key  $(pk_{A_1}, X_0)$  under which the ciphertext  $(Y, y_1, y_0)$  is computed, while  $X$  is part of the ciphertext  $(X, x_1)$  under public key  $E_{B_2}$  (we omit  $Y$ ). The other solution is to strengthen the underlying assumption as 1-Oracle SI-DH assumption such that  $h(j(E_X / \langle R_2 + [y]S_2 \rangle))$  could be leaked.

In consequence, the two solutions lead to two AKEs, namely,  $\text{SIAKE}_2$  and  $\text{SIAKE}_3$ .

- SOLUTION 1: We add an extra  $X_0$  to take the position of  $X$  as part of the public key  $(pk_{A_1}, X_0)$  under which the ciphertext  $(Y, y_1, y_0)$  is computed, remove  $x_2$  and set  $(X, x_1)$  as the ciphertext under public key  $E_{B_2}$  rather than  $(E_{B_2}, Y)$ . Then the value of  $h(j(E_X / \langle R_2 + [y]S_2 \rangle))$  is not needed during the security proof. The drawback of this solution is that  $K'_A$  can not be included in the session state of  $U_B$ . Solution 1 leads to  $\text{SIAKE}_2$ .
- SOLUTION 2: We strengthen the underlying SI-DDH assumption to the 1-Oracle SI-DH assumption to allow the leakage of  $h(j(E_X / \langle R_2 + [y]S_2 \rangle))$ . The 1-Oracle SI-DH assumption can be considered as a hashed SI-DDH assumption where a one-time hashed SI-CDH oracle is allowed. Note that considering  $\langle R_2 + [y]S_2 \rangle = \langle [u]R_2 + [y][u]S_2 \rangle$  for any integer  $1 \leq u \leq \ell_2^2$  and coprime to  $\ell_2$ , we employ a simple trick of tailoring the hash function as  $h(Y, j(E_{XY}))$  in  $x_2$  and  $h(X, j(E_{XY}))$  in  $y_2$ . This solution results in  $\text{SIAKE}_3$ .

### 1.3 Related Works and Their Analysis

Galbraith [15] proposed two SIDH variants of AKE, namely, Gal 1 from Jeong-Katz-Lee protocol [21] and Gal 2 from NAXOS protocol [27]. Considering the adaptive attack on static secret keys, Gal 1 protocol only allows honest registrants of static public keys and it is also vulnerable to the KCI attack. So far, neither has there been any concrete MEX attack on Gal 1, nor any formal proofs to show Gal 1 is resistant to the MEX attack. Gal 2 protocol is provably secure in BR model, which only allows honest registrants of static public keys (if the adversary gets the ephemeral secret key, like  $x$ , the adaptive attack still works), and can not resist the MEX attack.

Very recently, Fujioka et al. [14] gave two Diffie-Hellman like isogeny-based AKEs, namely, FTTY 1 and FTTY 2. FTTY 1 protocol, which is quite similar to Gal 1 scheme, is CK secure in the quantum random oracle model, but it only allows honest registrants and cannot resist the KCI attack. FTTY 2 is secure in  $\text{CK}^+$  model, but it also only allows honest registrants.

Below we illustrate in detail the (in)capability of Gal 1-2 and FTTY 1-2 on resisting the adaptive attacks (if the arbitrary registrant is allowed), the KCI attack, and the MEX attack.

**Adaptive attacks if *arbitrary* registrant is allowed.** Suppose that in a protocol Alice sets  $E_{A_1}, \phi_{A_1}(P_2), \phi_{A_1}(Q_2)$  as her static public key. The goal of a malicious adversary is to compute Alice’s static secret key. As illustrated in Figure 1, the session key of Gal 1 is extracted from  $E_{XY}$  and  $E_{A_1B_2}$ . By applying the adaptive attacks [17], a malicious adversary can register  $(E_{B_2}, R', S')$  with specified points  $R'$  and  $S'$ , rather than  $\phi_{B_2}(P_1)$  and  $\phi_{B_2}(Q_1)$ , as the static public key for Bob. By checking whether the session key computed by Alice (which can be obtained from `SessionKeyReveal` query) is equal to that computed by Bob, one bit of Alice’s static secret key is determined. The adversary gradually learns Alice’s static secret key by registering several valid static public keys according

to adaptive attacks. Such an attack can be applied to FTTY 1 directly and it also works for FTTY 2 if the adversary also has the ephemeral secret key  $x$  of Alice (which can be obtained by querying `SessionStateReveal`), which means that FTTY 2 also does not allow arbitrary registrant. Gal 2 does not allow arbitrary registrant either, since if the adversary has the ephemeral secret key  $x$  of Alice (which can be obtained from `SessionStateReveal` query), by honestly registering static public key for Bob, then sending  $(E_Y, R', S')$  with specified points  $R'$  and  $S'$ , and checking whether the session key computed by Alice is equal to that computed by Bob, the adversary is able to learn one bit of Alice's static secret key.

**KCI Attacks.** KCI attacks state that if a static secret key is revealed, an adversary can try to impersonate any other honest parties in order to fool the owners of the exposed secret keys. Neither Gal 1 nor FTTY 1 are resistant to the KCI attack since each session key is extracted from  $E_{XY}$  and  $E_{A_1B_2}$ , and by generating  $E_Y, \phi_Y(P_1), \phi_Y(Q_1)$  and sending it to Alice on behalf of Bob, with Alice's static secret key the adversary could compute the session key even if Bob's static secret key is unknown.

**MEX Attacks.** In MEX, an adversary aims to distinguish the session key from a random value under the disclosure of the ephemeral secret key of (at least) one party of the test session. Gal 2 is not resistant to the MEX attack since its session key is extracted from  $E_{XY}, E_{XB_2}$ , and  $E_{A_1Y}$ , thus it is easy for an adversary to compute those curves with the ephemeral secret key corresponding to  $E_X$  and  $E_Y$ .

## 2 Preliminaries

### 2.1 SIDH and Crypto-friendly Description

We recall briefly the SIDH protocol using the same notation as [8,20]. Let  $p$  be a large prime of the form  $p = \ell_1^{e_1} \ell_2^{e_2} \cdot f \pm 1$ , where  $\ell_1$  and  $\ell_2$  are two small primes, and  $f$  is an integer cofactor. Then we can construct a supersingular elliptic curve  $E_0$  defined over  $\mathbb{F}_{p^2}$  with order  $|E_0(\mathbb{F}_{p^2})| = (\ell_1^{e_1} \ell_2^{e_2} \cdot f)^2$ . Let  $\mathbb{Z}_m$  be the ring of residue classes modulo  $m$ . The subgroup  $E_0[m]$  of  $m$ -torsion points is isomorphic to  $\mathbb{Z}_m \times \mathbb{Z}_m$  for  $m \in \{\ell_1^{e_1}, \ell_2^{e_2}\}$ . Let  $P_1, Q_1$  be two points that generate  $E_0[\ell_1^{e_1}]$  and  $P_2, Q_2$  be two points that generate  $E_0[\ell_2^{e_2}]$ . The public parameters are  $(E_0; P_1, Q_1; P_2, Q_2; \ell_1, \ell_2, e_1, e_2)$ .

The SIDH, as depicted in Figure 2, works as follows. Alice chooses her secret key  $k_a$  from  $\mathbb{Z}_{\ell_1^{e_1}}$  and computes the isogeny  $\phi_A : E_0 \rightarrow E_A$  whose kernel is the subgroup  $\langle R_A \rangle = \langle P_1 + [k_a]Q_1 \rangle$ . She then sends to Bob her public key which is  $E_A$  together with the two points  $\phi_A(P_2), \phi_A(Q_2)$ . Similarly, Bob chooses his secret key  $k_b$  from  $\mathbb{Z}_{\ell_2^{e_2}}$  and computes the isogeny  $\phi_B : E_0 \rightarrow E_B$  with kernel subgroup  $\langle R_B \rangle = \langle P_2 + [k_b]Q_2 \rangle$ . He sends to Alice his public key which is  $E_B$  together with the two points  $\phi_B(P_1), \phi_B(Q_1)$ . To get the shared secret, Alice computes the isogeny  $\phi_{BA} : E_B \rightarrow E_{BA}$  with kernel subgroup generated by

$$\begin{array}{ccc}
E_0 & \xrightarrow{\phi_A} & E_A = E_0/\langle R_A \rangle \\
\downarrow \phi_B & & \downarrow \phi_{AB} \\
E_B = E_0/\langle R_B \rangle & \xrightarrow{\phi_{BA}} & E_{AB} = E_0/\langle R_A, R_B \rangle
\end{array}$$

**Fig. 2.** SIDH

$\phi_B(P_1) + [k_a]\phi_B(Q_1)$ . Similarly, Bob computes the isogeny  $\phi_{AB} : E_A \rightarrow E_{AB}$  with kernel subgroup generated by  $\phi_A(P_2) + [k_b]\phi_A(Q_2)$ . Since the composed isogeny  $\phi_{AB} \circ \phi_A$  has the same kernel  $\langle R_A, R_B \rangle$  as  $\phi_{BA} \circ \phi_B$ , Alice and Bob can share the same  $j$ -invariant  $j(E_{AB}) = j(E_{BA})$ .

It will be helpful to have a crypto-friendly description of SIDH for the presentation of our AKEs. We follow the treatment of Fujioka et al. [14]. In what follows we assume  $\{t, s\} = \{1, 2\}$ , and denote the public parameters by  $\mathbf{g} = (E_0; P_1, Q_1, P_2, Q_2)$  and  $\mathbf{e} = (\ell_1, \ell_2, e_1, e_2)$ . We define the sets of supersingular curves and those with an auxiliary basis as

$$\begin{aligned}
\text{SSEC}_p &= \{\text{supersingular elliptic curves } E \text{ over } \mathbb{F}_{p^2} \text{ with } E(\mathbb{F}_{p^2}) \simeq (\mathbb{Z}_{\ell_1^{e_1} \ell_2^{e_2} f})^2\}; \\
\text{SSEC}_A &= \{(E; P'_t, Q'_t) \mid E \in \text{SSEC}_p, (P'_t, Q'_t) \text{ is basis of } E[\ell_t^{e_t}]\}; \\
\text{SSEC}_B &= \{(E; P'_s, Q'_s) \mid E \in \text{SSEC}_p, (P'_s, Q'_s) \text{ is basis of } E[\ell_s^{e_s}]\}.
\end{aligned}$$

Let  $\mathbf{a} = k_a$  and  $\mathbf{b} = k_b$ , then we define,

$$\begin{aligned}
\mathbf{g}^{\mathbf{a}} &= (E_A; \phi_A(P_t), \phi_A(Q_t)) \in \text{SSEC}_A, \\
&\quad \text{where } R_A = P_s + [k_a]Q_s, \phi_A : E_0 \rightarrow E_A = E_0/\langle R_A \rangle; \\
\mathbf{g}^{\mathbf{b}} &= (E_B; \phi_B(P_s), \phi_B(Q_s)) \in \text{SSEC}_B, \\
&\quad \text{where } R_B = P_t + [k_b]Q_t, \phi_B : E_0 \rightarrow E_B = E_0/\langle R_B \rangle; \\
(\mathbf{g}^{\mathbf{b}})^{\mathbf{a}} &= j(E_{BA}), \text{ where } R_{BA} = \phi_B(P_s) + [k_a]\phi_B(Q_s), \\
&\quad \phi_{BA} : E_B \rightarrow E_{BA} = E_B/\langle R_{BA} \rangle; \\
(\mathbf{g}^{\mathbf{a}})^{\mathbf{b}} &= j(E_{AB}), \text{ where } R_{AB} = \phi_A(P_t) + [k_b]\phi_A(Q_t), \\
&\quad \phi_{AB} : E_A \rightarrow E_{AB} = E_A/\langle R_{AB} \rangle.
\end{aligned}$$

Using this notation, the SIDH looks almost exactly like the classical Diffie-Hellman. That is, the public parameters are  $\mathbf{g}$  and  $\mathbf{e}$ . Alice chooses a secret key  $\mathbf{a}$  and sends  $\mathbf{g}^{\mathbf{a}}$  to Bob, while Bob chooses a secret key  $\mathbf{b}$  and sends  $\mathbf{g}^{\mathbf{b}}$  to Alice. The shared key is, as we expect,  $j = (\mathbf{g}^{\mathbf{b}})^{\mathbf{a}} = (\mathbf{g}^{\mathbf{a}})^{\mathbf{b}}$ .

## 2.2 Standard SIDH Assumptions

We describe two standard assumptions about supersingular isogeny based on the crypto-friendly notation. Let  $s \neq t$  and  $s, t \in \{1, 2\}$ .

**Definition 1 (SI-CDH Assumption [8,14]).** *The SI-CDH problem is that, given public parameters  $\mathbf{g}$  and  $\mathbf{e}$ , and  $\mathbf{g}^{\mathbf{a}}$ ,  $\mathbf{g}^{\mathbf{b}}$  where  $\mathbf{a} \leftarrow \mathbb{Z}_{\ell_s^{e_s}}$ ,  $\mathbf{b} \leftarrow \mathbb{Z}_{\ell_t^{e_t}}$ , compute the  $j$ -invariant  $(\mathbf{g}^{\mathbf{a}})^{\mathbf{b}} = (\mathbf{g}^{\mathbf{b}})^{\mathbf{a}}$ . For any PPT algorithm  $\mathcal{A}$ , we define the advantage of solving SI-CDH problem as*

$$Adv_{\mathcal{A}}^{sicdh} = Pr[j' = (\mathbf{g}^{\mathbf{a}})^{\mathbf{b}} | j' \leftarrow \mathcal{A}(\mathbf{g}, \mathbf{e}, \mathbf{g}^{\mathbf{a}}, \mathbf{g}^{\mathbf{b}})].$$

*The SI-CDH assumption states: for any PPT algorithm  $\mathcal{A}$ , the advantage of solving SI-CDH problem is negligible.*

**Definition 2 (SI-DDH Assumption [8,14]).** *Let  $\mathbf{g}$  and  $\mathbf{e}$  be that defined in SI-CDH assumption. Let  $D_0$  and  $D_1$  be two distributions defined as:*

$$D_1 := \{\mathbf{e}, \mathbf{g}, \mathbf{g}^{\mathbf{a}}, \mathbf{g}^{\mathbf{b}}, (\mathbf{g}^{\mathbf{a}})^{\mathbf{b}} | \mathbf{a} \leftarrow \mathbb{Z}_{\ell_s^{e_s}}, \mathbf{b} \leftarrow \mathbb{Z}_{\ell_t^{e_t}}\}$$

$$D_0 := \{\mathbf{e}, \mathbf{g}, \mathbf{g}^{\mathbf{a}}, \mathbf{g}^{\mathbf{b}}, (\mathbf{g}^{\mathbf{s}})^{\mathbf{t}} | \mathbf{a}, \mathbf{s} \leftarrow \mathbb{Z}_{\ell_s^{e_s}}, \mathbf{b}, \mathbf{t} \leftarrow \mathbb{Z}_{\ell_t^{e_t}}\}$$

*The SI-DDH problem is that given a random sample from  $D_b$  depending on  $b \leftarrow \{0, 1\}$ , guess  $b$ . The advantage of solving SI-DDH problem for any PPT algorithm  $\mathcal{A}$  is*

$$Adv_{\mathcal{A}}^{siddh} = Pr[b' = b | b' \leftarrow \mathcal{A}(\mathfrak{d}_b \leftarrow D_b), b \leftarrow \{0, 1\}] - 1/2.$$

*The SI-DDH assumption states: for any PPT algorithm  $\mathcal{A}$ , the advantage of solving SI-DDH problem is negligible.*

### 2.3 CK<sup>+</sup> Security Model

We recall the CK<sup>+</sup> model introduced by [22] and later refined by [12], which is a CK model [6] integrated with the weak PFS, resistance to KCI and MEX properties. We focus on 3-pass and 2-pass protocols in this paper. For simplicity, we only show the model specified to 2-pass protocols. As for 3-pass protocol, we can extend it by adding an extra message in the matching session identifier and Send definitions.

In an AKE protocol,  $U_i$  denotes a party indexed by  $i$ , who is modeled as a probabilistic polynomial time (PPT) interactive Turing machine. We assume that each party  $U_i$  owns a static pair of secret-public key  $(sk_i, pk_i)$ , where the static public key is related to  $U_i$ 's identity by a certification authority (CA). No other actions by the CA are required or assumed. In particular, we make no assumption on whether the CA requires a proof-of possession of the private key from a registrant of a public key, and we do not assume any specific checks on the value of a public key.

**Session.** Each party can be activated to run an instance called a *session*. A party can be activated to initiate the session by an incoming message of the form  $(\Pi, \mathcal{I}, U_A, U_B)$  or respond to an incoming message of the form  $(\Pi, \mathcal{R}, U_B, U_A, X_A)$ , where  $\Pi$  is a protocol identifier,  $\mathcal{I}$  and  $\mathcal{R}$  are role identifiers corresponding to *initiator* and *responder*. Activated with  $(\Pi, \mathcal{I}, U_A, U_B)$ ,  $U_A$  is called the session *initiator*. Activated with  $(\Pi, \mathcal{R}, U_B, U_A, X_A)$ ,  $U_B$  is called the session *responder*.

According to the specification of AKE, the party creates randomness which is generally called *ephemeral secret key*, computes and maintains a *session state*, generates outgoing messages, and completes the session by outputting a session key and erasing the session state. Note that Canetti-Krawczyk [6] defines session state as session-specific secret information, but leaves it up to a protocol to specify which information is included in a session state. LaMacchia et al. [27] explicitly set all random coins used by a party in a session as session-specific secret information and call it *ephemeral secret key*. Here we require that the session state at least contains the ephemeral secret key.

A session may also be aborted without generating a session key. The initiator  $U_A$  creates a session state and outputs  $X_A$ , then may receive an incoming message of the forms  $(\Pi, \mathcal{I}, U_A, U_B, X_A, X_B)$  from the responder  $U_B$ , and may compute the session key  $SK$ . On the contrary, the responder  $U_B$  outputs  $X_B$ , and may compute the session key  $SK$ . We say that a session is *completed* if its owner computes the session key.

A session is associated with its owner, a peer, and a session identifier. If  $U_A$  is the initiator, the session identifier is  $\text{sid} = (\Pi, \mathcal{I}, U_A, U_B, X_A)$  or  $\text{sid} = (\Pi, \mathcal{I}, U_A, U_B, X_A, X_B)$ , which denotes  $U_A$  as an owner and  $U_B$  as a peer. If  $U_B$  is the responder, the session is identified by  $\text{sid} = (\Pi, \mathcal{R}, U_B, U_A, X_A, X_B)$ , which denotes  $U_B$  as an owner and  $U_A$  as a peer. The *matching session* of  $(\Pi, \mathcal{I}, U_A, U_B, X_A, X_B)$  is  $(\Pi, \mathcal{R}, U_B, U_A, X_A, X_B)$  and vice versa.

**Adversary.** Adversary  $\mathcal{A}$  is modeled as follows to capture real attacks in open networks, including the control of communication and the access to some of the secret information.

- **Send(message):**  $\mathcal{A}$  sends messages in one of the forms:  $(\Pi, \mathcal{I}, U_A, U_B)$ ,  $(\Pi, \mathcal{R}, U_B, U_A, X_A)$ , or  $(\Pi, \mathcal{I}, U_A, U_B, X_A, X_B)$ , and obtains the response.
- **SessionKeyReveal(sid):** if the session  $\text{sid}$  is completed,  $\mathcal{A}$  obtains the session key  $SK$  for  $\text{sid}$ .
- **SessionStateReveal(sid):**  $\mathcal{A}$  obtains the session state of the owner of  $\text{sid}$  if the session is not completed. The session state includes all ephemeral secret keys and intermediate computation results except for immediately erased information, but does not include the static secret key.
- **Corrupt( $U_i$ ):** By this query,  $\mathcal{A}$  learns all information of  $U_A$  (including the static secret, session states and session keys stored at  $U_A$ ). In addition, from the moment that  $U_A$  is corrupted, all its actions may be controlled by  $\mathcal{A}$ .

**Freshness.** Let  $\text{sid}^* = (\Pi, \mathcal{I}, U_A, U_B, X_A, X_B)$  or  $(\Pi, \mathcal{I}, U_A, U_B, X_A, X_B)$  be a completed session between honest users  $U_A$  and  $U_B$ . If the matching session of  $\text{sid}^*$  exists, denote it by  $\overline{\text{sid}}^*$ . We say session  $\text{sid}^*$  is fresh if  $\mathcal{A}$  does not query: 1) **SessionStateReveal( $\text{sid}^*$ )**, **SessionKeyReveal( $\text{sid}^*$ )**, and **SessionStateReveal( $\overline{\text{sid}}^*$ )**, **SessionKeyReveal( $\overline{\text{sid}}^*$ )** if  $\overline{\text{sid}}^*$  exists; 2) **SessionStateReveal( $\text{sid}^*$ )** and **SessionKeyReveal( $\text{sid}^*$ )** if  $\overline{\text{sid}}^*$  does not exist.

**Security Experiment.** The adversary  $\mathcal{A}$  could make a sequence of the queries described above. During the experiment,  $\mathcal{A}$  makes the query of **Test( $\text{sid}^*$ )**, where  $\text{sid}^*$  must be a fresh session. **Test( $\text{sid}^*$ )** select random bit  $b \in \{0, 1\}$ , and return

the session key held by  $\text{sid}^*$  if  $b = 0$ ; and return a random key if  $b = 1$ . The experiment continues until  $\mathcal{A}$  returns  $b'$  as a guess of  $b$ . The adversary  $\mathcal{A}$  wins the game if the test session  $\text{sid}^*$  is still fresh and  $b' = b$ . The advantage of the adversary  $\mathcal{A}$  is defined as  $\text{Adv}_{\Pi}^{\text{ck}^+}(\mathcal{A}) = \Pr[\mathcal{A} \text{ wins}] - \frac{1}{2}$ .

**Definition 3.** We say that a AKE protocol  $\Pi$  is secure in the  $\text{CK}^+$  model if the following conditions hold:

**Correctness:** If two honest parties complete matching sessions, then they both compute the same session key except with negligible probability.

**Soundness:** For any PPT adversary  $\mathcal{A}$ ,  $\text{Adv}_{\Pi}^{\text{CK}^+}(\mathcal{A})$  is negligible for the test session  $\text{sid}^*$ ,

1. the static secret key of the owner of  $\text{sid}^*$  is given to  $\mathcal{A}$ , if  $\overline{\text{sid}}^*$  does not exist.
2. the ephemeral secret key of the owner of  $\text{sid}^*$  is given to  $\mathcal{A}$ , if  $\overline{\text{sid}}^*$  does not exist.
3. the static secret key of the owner of  $\text{sid}^*$  and the ephemeral secret key of  $\overline{\text{sid}}^*$  are given to  $\mathcal{A}$ , if  $\overline{\text{sid}}^*$  exists.
4. the ephemeral secret key of  $\text{sid}^*$  and the ephemeral secret key of  $\overline{\text{sid}}^*$  are given to  $\mathcal{A}$ , if  $\overline{\text{sid}}^*$  exists.
5. the static secret key of the owner of  $\text{sid}^*$  and the static secret key of the peer of  $\text{sid}^*$  are given to  $\mathcal{A}$ , if  $\overline{\text{sid}}^*$  exists.
6. the ephemeral secret key of  $\text{sid}^*$  and the static secret key of the peer of  $\text{sid}^*$  are given to  $\mathcal{A}$ , if  $\overline{\text{sid}}^*$  exists.

As indicated in Table 2, the  $\text{CK}^+$  model captures all non-trivial patterns of exposure of static and ephemeral secret keys listed in Definition 3, and these ten cases cover wPFS, resistance to KCI, and MEX attacks.

Event	Case	$\text{sid}^*$	$\overline{\text{sid}}^*$	$sk_A$	$ek_A$	$ek_B$	$sk_B$	Security
$E_1$	1	$A$	No	$\sqrt{\quad}$	$\times$	-	$\times$	KCI
$E_2$	2	$A$	No	$\times$	$\sqrt{\quad}$	-	$\times$	MEX
$E_3$	2	$B$	No	$\times$	-	$\sqrt{\quad}$	$\times$	MEX
$E_4$	1	$B$	No	$\times$	-	$\times$	$\sqrt{\quad}$	KCI
$E_5$	5	$A$ or $B$	Yes	$\sqrt{\quad}$	$\times$	$\times$	$\sqrt{\quad}$	wPFS
$E_6$	4	$A$ or $B$	Yes	$\times$	$\sqrt{\quad}$	$\sqrt{\quad}$	$\times$	MEX
$E_{7-1}$	3	$A$	Yes	$\sqrt{\quad}$	$\times$	$\sqrt{\quad}$	$\times$	KCI
$E_{7-2}$	3	$B$	Yes	$\times$	$\sqrt{\quad}$	$\times$	$\sqrt{\quad}$	KCI
$E_{8-1}$	6	$A$	Yes	$\times$	$\sqrt{\quad}$	$\times$	$\sqrt{\quad}$	KCI
$E_{8-2}$	6	$B$	Yes	$\sqrt{\quad}$	$\times$	$\sqrt{\quad}$	$\times$	KCI

**Table 2.** The behavior of AKE adversary in  $\text{CK}^+$  model.  $\overline{\text{sid}}^*$  is the matching session of  $\text{sid}^*$ , if it exists. “Yes” means that there exists  $\overline{\text{sid}}^*$  and “No” means not.  $sk_A$  (resp.  $sk_B$ ) means the static secret key of  $A$  (resp.  $B$ ).  $ek_A$  (resp.  $ek_B$ ) is the ephemeral secret key of  $A$  (resp.  $B$ ) in  $\text{sid}^*$  or  $\overline{\text{sid}}^*$  if there exists. “ $\sqrt{\quad}$ ” means the secret key may be revealed to adversary, “ $\times$ ” means the secret key is not revealed. “-” means the secret key does not exist.

## 2.4 2-Key PKE and KEM

In this section, we provide the definitions of 2-key PKE and 2-key KEM, as well as the modified Fujisaki-Okamoto transformation proposed by Xue et al. [34].

A 2-key PKE with a plaintext space  $\mathcal{M}$  and a ciphertext space  $\mathcal{C}$  consists of a quadruple of PPT algorithms  $2\text{PKE}=(\text{KeyG1}, \text{KeyG0}, \text{Enc}, \text{Dec})$  described as follows:

- $\text{KeyG1}(n, pp)$  : on input a security parameter  $n$  and public parameter  $pp$ , output a pair of public and secret keys  $(pk_1, sk_1)$ .
- $\text{KeyG0}(n, pp)$  : on input a security parameter  $n$  and public parameter  $pp$ , output a pair of public and secret keys  $(pk_0, sk_0)$ .
- $\text{Enc}(pk_1, pk_0, m; r)$  : on input public keys  $pk_1, pk_0$  and a plaintext  $m \in \mathcal{M}$ , output a ciphertext  $C \in \mathcal{C}$ .
- $\text{Dec}(sk_1, sk_0, C)$  : on input secret keys  $sk_1, sk_0$  and a ciphertext  $C \in \mathcal{C}$ , output a plaintext  $m$ .

CORRECTNESS. For  $(pk_1, sk_1) \leftarrow \text{KeyG1}(n, pp)$ ,  $(pk_0, sk_0) \leftarrow \text{KeyG0}(n, pp)$  and  $C \leftarrow \text{Enc}(pk_1, pk_0, m; r)$ , then we have  $\text{Dec}(sk_1, sk_0, C) = m$ .

Game [OW-CPA, $\cdot$ ] on $pk_1$	Game [ $\cdot$ , OW-CPA] on $pk_0$
01 $(pk_1, sk_1) \leftarrow \text{KeyG1}(n, pp)$ ;	07 $(pk_0, sk_0) \leftarrow \text{KeyG0}(n, pp)$ ;
02 $(state, pk_0^*) \leftarrow \mathcal{A}_1(pk_1)$ ;	08 $(state, pk_1^*) \leftarrow \mathcal{B}_1(pk_0)$ ;
03 $m \leftarrow \mathcal{M}$ ;	09 $m \leftarrow \mathcal{M}$ ;
04 $c^* \leftarrow \text{Enc}(pk_1, pk_0^*, m)$ ;	10 $c^* \leftarrow \text{Enc}(pk_1^*, pk_0, m)$ ;
05 $m' \leftarrow \mathcal{A}_2(state, c^*)$ ;	11 $m' \leftarrow \mathcal{B}_2(state, c^*)$ ;
06 return $m' \stackrel{?}{=} m$	12 return $m' \stackrel{?}{=} m$

**Fig. 3.** The [OW-CPA,  $\cdot$ ] (resp. [ $\cdot$ , OW-CPA]) game of 2PKE for adversaries  $\mathcal{A}$  (resp.  $\mathcal{B}$ ).

The security games of 2PKE are formalized in Figure 3. We define the advantage of  $\mathcal{A}$  winning in the game [OW-CPA,  $\cdot$ ] as  $\text{Adv}_{2\text{PKE}}^{[\text{OW-CPA}, \cdot]}(\mathcal{A}) = \Pr[[\text{OW-CPA}, \cdot]^{\mathcal{A}} \Rightarrow 1]$ , and the advantage of  $\mathcal{B}$  in the game [ $\cdot$ , OW-CPA] as  $\text{Adv}_{2\text{PKE}}^{[\cdot, \text{OW-CPA}]}(\mathcal{B}) = \Pr[[\cdot, \text{OW-CPA}]^{\mathcal{B}} \Rightarrow 1]$ , respectively.

The 2-key key encapsulation (2-key KEM) 2KEM is defined similarly.

- $\text{KeyGen1}(n, pp)$  : on input a security parameter  $n$  and public parameter  $pp$ , output a pair of public-secret keys  $(pk_1, sk_1)$ . In order to show the randomness that is used, we denote key generation algorithm as  $\text{KeyGen1}(n, r)$ .
- $\text{KeyGen0}(n, pp)$  : on input a security parameter  $n$  and public parameter  $pp$ , output a pair of public and secret keys  $(pk_0, sk_0)$ .
- $\text{Encaps}(pk_1, pk_0)$  : on input public keys  $pk_1, pk_0$ , output a ciphertext  $c$  and encapsulated key  $k$  in key space  $\mathcal{K}$ . Sometimes, we explicitly add the randomness  $r$  and denote it as  $\text{Encaps}(pk_1, pk_0; r)$ .
- $\text{Decaps}(sk_1, sk_0, c)$  : on input secret keys  $sk_1, sk_0$  and a ciphertext  $c$ , output a key  $k$ .

CORRECTNESS. For  $(pk_1, sk_1) \leftarrow \text{KeyGen1}(n, pp)$ ,  $(pk_0, sk_0) \leftarrow \text{KeyGen0}(n, pp)$  and  $(c, k) \leftarrow \text{Encaps}(pk_1, pk_0)$ , it holds that  $\text{Decaps}(sk_1, sk_0, c) = k$ .

Game [OW-CCA, ·] on $pk_1$	Game [·, OW-CPA] on $pk_0$
01 $(pk_1, sk_1) \leftarrow \text{KeyGen1}(n, pp)$ ;	07 $(pk_0, sk_0) \leftarrow \text{KeyGen0}(n, pp)$ ;
02 $L_0 = \{(-, -, -)\}$ ;	08 $(state, pk_1^*) \leftarrow \mathcal{B}_1(pk_0)$ ;
03 $(state, pk_0^*) \leftarrow \mathcal{A}_1^{\mathcal{O}_{cca}, \mathcal{O}_{leak_0}}(pk_1)$ ;	09 $(c^*, k^*) \leftarrow \text{Encaps}(pk_1^*, pk_0)$ ;
04 $(c^*, k^*) \leftarrow \text{Encaps}(pk_1, pk_0^*)$ ;	10 $k' \leftarrow \mathcal{B}_2(state, c^*)$ ;
05 $k' \leftarrow \mathcal{A}_2^{\mathcal{O}_{cca}, \mathcal{O}_{leak_0}}(state, c^*)$ ;	11 return $k' \stackrel{?}{=} k^*$
06 return $k' \stackrel{?}{=} k^*$	

**Fig. 4.** The [OW-CCA, ·] (resp. [·, OW-CPA]) game of 2KEM for adversaries  $\mathcal{A}$  (resp.  $\mathcal{B}$ ). The oracles  $\mathcal{O}_{leak_0}$  and  $\mathcal{O}_{cca}$  are defined in the following.

The security games of 2KEM are formalized in Figure 4. On the  $i$ -th query of  $\mathcal{O}_{leak_0}$ , the challenger generates  $(pk_0^i, sk_0^i) \leftarrow \text{KeyGen0}(r_0^i)$ , sets  $L_0 = L_0 \cup \{(pk_0^i, sk_0^i)\}$  and returns  $(pk_0^i, sk_0^i)$  to adversary  $\mathcal{A}$ .  $\mathcal{O}_{cca}(pk_0^i, c')$  works as follows: If  $pk_0^i \in [L_0]_1$  and  $(c', pk_0^i) \neq (c^*, pk_0^*)$ , compute and return the corresponding  $k' \leftarrow \text{Decaps}(sk_1, sk_0^i, c')$ , otherwise return  $\perp$ .

We define the advantage of  $\mathcal{A}$  winning in the game [OW-CCA, ·] as

$$\text{Adv}_{2\text{KEM}}^{\text{[OW-CCA, ·]}}(\mathcal{A}) = \Pr[\text{[OW-CCA, ·]}^{\mathcal{A}} \Rightarrow 1],$$

and the advantage of  $\mathcal{B}$  winning in the game [·, OW-CPA] as:

$$\text{Adv}_{2\text{KEM}}^{\text{[·, OW-CPA]}}(\mathcal{B}) = \Pr[\text{[·, OW-CPA]}^{\mathcal{B}} \Rightarrow 1].$$

According to [34], the modified Fujisaki-Okamoto transformation in Fig. 5 builds a [OW-CCA, OW-CPA] secure 2-Key KEM from any [OW-CPA, OW-CPA] secure 2-key PKE. Note that in [34] they consider the decryption failure, but we do not take the decryption failure into account here since the encryption scheme based on SI-DDH is perfectly correct.

**Lemma 1 (Theorem 7 [34]).** *For any [OW-CCA, ·] adversary  $\mathcal{C}$ , or [·, OW-CPA] adversary  $\mathcal{D}$  against 2KEM with at most  $q_H$  queries to random oracle  $H$ , there are [OW-CPA, ·] adversary  $\mathcal{A}$ , or [·, OW-CPA] adversary  $\mathcal{B}$  against 2PKE, that make at most  $q_H$  (resp.  $q_G$ ) queries to random oracle  $H$  (resp.  $G$ ) s.t.*

$$\text{Adv}_{2\text{KEM}}^{\text{[OW-CCA, ·]}}(\mathcal{C}) \leq \frac{q_H}{2^n} + q_H \cdot \text{Adv}_{2\text{PKE}}^{\text{[OW-CPA, ·]}}(\mathcal{A}),$$

$$\text{Adv}_{2\text{KEM}}^{\text{[·, OW-CPA]}}(\mathcal{D}) \leq \text{Adv}_{2\text{PKE}}^{\text{[·, OW-CPA]}}(\mathcal{B}).$$

KeyGen1( $n$ )	KeyGen0( $n$ )
$(pk'_1, sk'_1) \leftarrow \text{KeyG1}$	$(pk'_0, sk'_0) \leftarrow \text{KeyG0}$
$s_1 \leftarrow \{0, 1\}^n$	$sk_0 = sk'_0$
$sk_1 = (sk'_1, s_1)$	$pk_0 = pk'_0$
$pk_1 = pk'_1$	return $(K, c)$
Encaps( $pk_1, pk_0$ );	Decaps( $sk_1, sk_0, c$ )
$m \leftarrow \mathcal{M}$	$m' = \text{Dec}(sk'_1, sk'_0, c)$
$c \leftarrow \text{Enc}(pk_1, pk_0, m; G(m))$	$c' = \text{Enc}(pk_1, pk_0, m'; G(m'))$
$K = H(pk_0, m, c)$	if $c \neq c'$ , let $m' = s_1$
return $(K, c)$	return $K = H(pk_0, m', c)$

**Fig. 5.** The modified Fujisaki-Okamoto from [OW-CPA, OW-CPA] secure 2-key PKE to [OW-CCA, OW-CPA] secure 2-key KEM 2KEM.

### 3 [OW-CCA, OW-CPA] Secure KEM from SIDH

We now propose a [OW-CCA, OW-CPA] secure 2-key KEM from supersingular isogeny. It is the core building block for our AKEs. At first, we propose a [OW-CPA, OW-CPA] 2-key PKE from supersingular isogeny, and then apply the modified Fujisaki-Okamoto transformation to obtain a 2-key KEM.

Choose  $p = \ell_1^{e_1} \ell_2^{e_2} \cdot f \pm 1, E_0, \{P_1, Q_1\}, \{P_2, Q_2\}$  as above. Let  $h : \{0, 1\}^* \rightarrow \{0, 1\}^n$  be a random hash function from pair-wise independent hash function families  $\mathcal{H}$ . Let  $\mathbf{g} = (E_0; P_1, Q_1, P_2, Q_2)$  and  $\mathbf{e} = (\ell_1, \ell_2, e_1, e_2)$  be public parameters. Let  $\{s, t\} = \{1, 2\}$ . The [OW-CPA, OW-CPA] 2-key PKE  $2\text{PKE}_{sidh}$  is built as follows.

- $\text{KeyG1}(n, \text{pp})$ : on input security parameter and public parameter, randomly choose a secret  $\mathbf{a}_1 \leftarrow \mathbb{Z}_{\ell_s^{e_s}}$  and compute  $\mathbf{g}^{\mathbf{a}_1}$ . Then output

$$sk_1 := \mathbf{a}_1, pk_1 := \mathbf{g}^{\mathbf{a}_1}.$$

- $\text{KeyG0}(n, \text{pp})$ : on input security parameter and public parameter, randomly choose a secret  $\mathbf{a}_0 \leftarrow \mathbb{Z}_{\ell_s^{e_s}}$  and compute  $\mathbf{g}^{\mathbf{a}_0}$ . Then output

$$sk_0 := \mathbf{a}_0, pk_0 := \mathbf{g}^{\mathbf{a}_0}.$$

- $\text{Enc}(pk_1, pk_0, m)$ : on input public keys and a message  $m = m_1 || m_0 \in \{0, 1\}^{2n}$ , randomly choose  $\mathbf{b} \leftarrow \mathbb{Z}_{\ell_t^{e_t}}$  and compute  $\mathbf{g}^{\mathbf{b}}, h((\mathbf{g}^{\mathbf{a}_1})^{\mathbf{b}}) \oplus m_1$  and  $h((\mathbf{g}^{\mathbf{a}_0})^{\mathbf{b}}) \oplus m_0$ . The ciphertext is

$$c := (\mathbf{g}^{\mathbf{b}}, h((\mathbf{g}^{\mathbf{a}_1})^{\mathbf{b}}) \oplus m_1, h((\mathbf{g}^{\mathbf{a}_0})^{\mathbf{b}}) \oplus m_0).$$

- $\text{Dec}(sk_1, sk_0, c)$ : on input secret keys  $sk_1 = \mathbf{a}_1, sk_0 = \mathbf{a}_0$  and ciphertext  $c = (c_1, c_2, c_3)$ , compute  $m_1 := c_2 \oplus h(c_1^{\mathbf{a}_1})$  and  $m_0 := c_3 \oplus h(c_1^{\mathbf{a}_0})$ . The plaintext is  $m = m_1 || m_0$ .

The correctness of  $2\text{PKE}_{sidh}$  is straightforward due to the correctness of SIDH.

**Lemma 2.** *Under the SI-DDH assumption,  $2PKE_{sidh}$  is [OW-CPA, OW-CPA] secure. Precisely, for any PPT [OW-CPA, ·] (resp. [·, OW-CPA]) adversary  $\mathcal{A}$  (resp.  $\mathcal{C}$ ), there exists algorithm  $\mathcal{B}$  (resp.  $\mathcal{D}$ ) such that*

$$\begin{aligned} Adv_{2PKE_{sidh}}^{[OW-CPA, \cdot]}(\mathcal{A}) &\leq 2Adv_{\mathcal{B}}^{siddh} + 1/2^n + \text{negl}, \\ (\text{resp. } Adv_{2PKE_{sidh}}^{[\cdot, OW-CPA]}(\mathcal{C}) &\leq 2Adv_{\mathcal{D}}^{siddh} + 1/2^n + \text{negl}). \end{aligned}$$

*Proof.* We reduce the [OW-CPA, ·] security to the underlying SI-DDH assumption. It is analogous for the [·, OW-CPA] security. We prove the [OW-CPA, ·] security via a sequence of games.

**Game 0:** This is the original [OW-CPA, ·] challenge game in Fig. 3. We denote the event that the adversary wins the games as  $\text{Succ}_0$ .

**Game 1:** In this game we modify [OW-CPA, ·] challenge game by requiring that the adversary wins the game if  $m'_1 = m_1$ . We denote this event as  $\text{Succ}_1$  (In Game  $i$  ( $i \geq 1$ ), we denote this event as  $\text{Succ}_i$ ). Note that in Game 0, the adversary wins only if both  $m'_1 = m_1$  and  $m'_0 = m_0$ . Thus, we have  $\Pr[\text{Succ}_0] \leq \Pr[\text{Succ}_1]$ .

**Game 2:** In this game, we modify the computation of challenge ciphertext. Specifically,  $(\mathbf{g}^b)^{a_1}$  is replaced by a random  $j$ -invariant  $j^*$ . We construct an algorithm  $\mathcal{B}$  to solve the SI-DDH problem given an instance  $(\mathbf{g}, \mathbf{g}_1, \mathbf{g}_2, j)$ , if there exists an algorithm  $\mathcal{A}$  to distinguish Game 1 and Game 2.

```


 $\mathcal{B}(\mathbf{e}, \mathbf{g}, \mathbf{g}_1, \mathbf{g}_2, j)$ 
01  $pk_1 \leftarrow \mathbf{g}_1$ 
02  $pk_0^*, \text{state} \leftarrow \mathcal{A}(pk_1)$ 
03  $m_1 \leftarrow \{0, 1\}^n$ 
04  $c_1^* = \mathbf{g}_2, c_2^* = h(j) \oplus m_1, c_3^* \leftarrow \{0, 1\}^n$ 
05  $c^* = (c_1^*, c_2^*, c_3^*)$ 
06  $m'_1 || m'_0 \leftarrow \mathcal{A}(\text{state}, c^*)$ 
07 If  $m'_1 = m_1, b' = 1$ , else  $b' \leftarrow \{0, 1\}$ .


```

If  $(\mathbf{g}, \mathbf{g}_1, \mathbf{g}_2, j)$  is an SI-DDH tuple,  $\mathcal{B}$  perfectly simulates Game 1, else  $\mathcal{B}$  perfectly simulates Game 2. In the SI-DDH challenge, we have

$$\begin{aligned} Adv_{\mathcal{B}}^{siddh} &= \Pr[b = b'] - 1/2 \\ &= 1/2(\Pr[b' = 1|b = 1] - \Pr[b' = 1|b = 0]) \\ &= 1/2(\Pr[b' = 1|\text{Game 1}] - \Pr[b' = 1|\text{Game 2}]) \\ &= 1/2(\Pr[\text{Succ}_1] - \Pr[\text{Succ}_2]). \end{aligned}$$

**Game 3:** In this game, we modify the computation of the challenge ciphertext. Specifically,  $h(j^*)$  is replaced by a random string  $h^*$ . Now  $c_2^*$  is a completely random string. Thus, the advantage to compute  $m_1$  is  $\Pr[\text{Succ}_3] = 1/2^n$ . Note that, since  $h$  is a pairwise independent hash function, by the leftover hash lemma,  $|\Pr[\text{Succ}_2] - \Pr[\text{Succ}_3]|$  is negligible.

To sum them up, we have that  $\Pr[\text{Succ}_0] \leq 2Adv_{\mathcal{B}}^{siddh} + 1/2^n + \text{negl}$ .  $\square$

**Remark 1:** By setting  $pk_0$  and  $sk_0$  to be empty and the ciphertext to be  $\mathbf{c}_1, \mathbf{c}_2$ , the scheme is exactly the ElGamal scheme and is OW-CPA secure under the SI-DDH assumption.

Applying the modified Fujisaki-Okamoto in Fig. 5, we get a [OW-CCA, OW-CPA] secure 2-key KEM  $2KEM_{sidh}$  in Fig. 6. Let  $G : \{0, 1\}^{2n} \rightarrow \{0, 1\}^*$  and  $H : \{0, 1\}^* \rightarrow \{0, 1\}^{2n}$  be hash functions. Note that there is a subtle difference between the Fig. 6 and the modified Fujisaki-Okamoto in Fig. 5 that the “re-encryption” only needs to check the correctness of  $\mathbf{c}_1$ .

KeyGen1	KeyGen0
$\mathbf{a}_1 \leftarrow \mathbb{Z}_{\ell_s}^{e_s}, s_1 \leftarrow \{0, 1\}^{2n}$	$\mathbf{a}_0 \leftarrow \mathbb{Z}_{\ell_s}^{e_s}$
$pk_1 := \mathbf{g}^{\mathbf{a}_1}, sk_1 := (\mathbf{a}_1, s_1)$	$pk_0 := \mathbf{g}^{\mathbf{a}_0}, sk_0 := \mathbf{a}_0$
Encaps( $pk_1, pk_0$ )	Decaps( $sk_1, sk_0$ )
$m_1, m_0 \leftarrow \{0, 1\}^n, \mathbf{b} := G(m_1, m_0)$	$m'_1 := c_2 \oplus h(\mathbf{c}_1^{\mathbf{a}_1})$
$\mathbf{c}_1 = \mathbf{g}^{\mathbf{b}}, c_2 = h((\mathbf{g}^{\mathbf{a}_1})^{\mathbf{b}}) \oplus m_1$	$m'_0 := c_3 \oplus h(\mathbf{c}_1^{\mathbf{a}_0})$
$c_3 = h((\mathbf{g}^{\mathbf{a}_0})^{\mathbf{b}}) \oplus m_0$	$\mathbf{b} := G(m'_1, m'_0)$
$c := (\mathbf{c}_1, c_2, c_3)$	If $\mathbf{c}_1 \neq \mathbf{g}^{\mathbf{b}}, m_1    m_0 = s_1$
$K := H(pk_0, m_1    m_0, c)$	$K := H(pk_0, m_1    m_0, c)$

**Fig. 6.** The [OW-CCA, OW-CPA] secure  $2KEM_{sidh}$ .

**Theorem 1.** *Under the SI-DDH assumption,  $2KEM_{sidh}$  is [OW-CCA, OW-CPA] secure in the random oracle model. Precisely, for any PPT [OW-CCA, ·] (resp. [·, OW-CPA]) adversary  $\mathcal{A}$  (resp.  $\mathcal{C}$ ) with at most  $q_H$  queries to  $H$  oracle, there exists algorithm  $\mathcal{B}$  (resp.  $\mathcal{D}$ ) solving SI-DDH problem such that*

$$Adv_{2KEM_{sidh}}^{[OW-CCA, \cdot]}(\mathcal{A}) \leq \frac{q_H}{2^{2n}} + q_H \cdot \left( 2Adv_{\mathcal{B}}^{sidh} + 1/2^n + negl \right),$$

$$(resp. Adv_{2KEM_{sidh}}^{[\cdot, OW-CPA]}(\mathcal{C}) \leq 2Adv_{\mathcal{D}}^{sidh} + 1/2^n + negl).$$

*Proof.* According to Lemma 1, the [OW-CCA, OW-CPA] security of  $2KEM_{sidh}$  is guaranteed by the [OW-CPA, OW-CPA] security of  $2PKE_{sidh}$ . By applying Lemma 2, the [OW-CCA, OW-CPA] security is finally reduced to the underlying SI-DDH assumption.  $\square$

**Remark 2:** By setting  $pk_0$  and  $sk_0$  to be empty, the message space to be  $\{0, 1\}^n$ , the input of  $G$  to be  $(m_1, -)$  and the ciphertext to be  $\mathbf{c}_1, \mathbf{c}_2$ , the scheme is exactly the FO transformed ElGamal scheme and is OW-CCA secure under the SI-DDH assumption.

## 4 Two-pass SIAKE

In this section, we propose a two-pass AKE based on SI-DDH assumption. The two-pass AKE SIAKE<sub>2</sub> is shown in Fig. 7.

$U_A$	$U_B$
$sk_{A_1} := (\mathbf{a}_1 \in \mathbb{Z}_{\ell_1^{e_1}}, s_{A_1} \leftarrow \{0, 1\}^{2n})$	$sk_{B_2} := (\mathbf{b}_2 \in \mathbb{Z}_{\ell_2^{e_2}}, s_{B_2} \leftarrow \{0, 1\}^{2n})$
$pk_{A_1} := \mathbf{g}^{\mathbf{a}_1}$	$pk_{B_2} := \mathbf{g}^{\mathbf{b}_2}$
$sk_{A_2} := (\mathbf{a}_2 \in \mathbb{Z}_{\ell_2^{e_2}}, s_{A_2} \leftarrow \{0, 1\}^{2n})$	$sk_{B_1} := (\mathbf{b}_1 \in \mathbb{Z}_{\ell_1^{e_1}}, s_{B_1} \leftarrow \{0, 1\}^{2n})$
$pk_{A_2} := \mathbf{g}^{\mathbf{a}_2}$	$pk_{B_1} := \mathbf{g}^{\mathbf{b}_1}$
$r_A \leftarrow \mathbb{Z}_{\ell_1^{e_1}}, n_1 \leftarrow g(r_A, \mathbf{a}_1)$	$r_B \leftarrow \mathbb{Z}_{\ell_2^{e_2}}, m_1    m_0 \leftarrow g(r_B, \mathbf{b}_2)$
$\mathfrak{r} \leftarrow G(n_1), \mathfrak{r}_0 \leftarrow \mathbb{Z}_{\ell_1^{e_1}}$	$\eta \leftarrow G(m_1, m_0)$
$X_0 := \mathbf{g}^{\mathfrak{r}_0}$	$Y := \mathbf{g}^\eta, y_1 := h((\mathbf{g}^{\mathbf{a}_1})^\eta) \oplus m_1$
$X := \mathbf{g}^{\mathfrak{r}}, x_1 := h((\mathbf{g}^{\mathbf{b}_2})^{\mathfrak{r}}) \oplus n_1$	$y_0 := h((\mathbf{g}^{\mathfrak{r}_0})^\eta) \oplus m_0$
$K_A := H(n_1, X, x_1)$	$K_B := H(X_0, m_1, m_0, Y, y_1, y_0)$
$m'_1 := y_1 \oplus h((\mathbf{g}^\eta)^{\mathbf{a}_1})$	$n'_1 := x_1 \oplus h((\mathbf{g}^{\mathfrak{r}})^{\mathbf{b}_2}), \mathfrak{r}' \leftarrow G(n'_1)$
$m'_0 := y_0 \oplus h((\mathbf{g}^\eta)^{\mathfrak{r}_0})$	$\text{If } X \neq \mathbf{g}^{\mathfrak{r}'}, n'_1 := s_{B_2}$
$\eta' \leftarrow G(m'_1, m'_0)$	$K'_A := H(n'_1, X, x_1)$
$\text{If } Y \neq \mathbf{g}^{\eta'}, m'_1    m'_0 := s_{A_1}$	$SK := \hat{H}(sid, K'_A, K_B)$
$K'_B := H(X_0, m'_1, m'_2, Y, y_1, y_0)$	
$SK := \hat{H}(sid, K_A, K'_B)$	

**Fig. 7.** A Compact 2-pass AKE SIAKE<sub>2</sub> Based on SI-DDH. Here *sid* is  $(U_A, U_B, pk_{A_1}, pk_{B_2}, X, x_1, X_0, Y, y_1, y_0)$ .

**Public Parameters:** Let  $\mathbf{e} = (\ell_1, \ell_2, e_1, e_2)$  and  $\mathbf{g} = (E_0; P_1, Q_1, P_2, Q_2)$ . Let  $g : \{0, 1\}^* \rightarrow \{0, 1\}^{2n}$ ,  $h : \{0, 1\}^n \rightarrow \{0, 1\}^n$ ,  $G : \{0, 1\}^{2n} \rightarrow \{0, 1\}^*$ ,  $H : \{0, 1\}^* \rightarrow \{0, 1\}^{2n}$ ,  $\hat{H} : \{0, 1\}^* \rightarrow \{0, 1\}^n$  be hash functions.

**Register:** Any user registers two sets of public-secret keys. One set of keys is assigned by the user as initiator, and another set is assigned as responder. For user  $U_A$ , it first chooses  $sk_{A_1} := (\mathbf{a}_1 \in \mathbb{Z}_{\ell_1^{e_1}}, s_{A_1} \leftarrow \{0, 1\}^{2n})$  and computes  $pk_{A_1} := \mathbf{g}^{\mathbf{a}_1}$ , then chooses  $sk_{A_2} := (\mathbf{a}_2 \in \mathbb{Z}_{\ell_2^{e_2}}, s_{A_2} \leftarrow \{0, 1\}^{2n})$  and computes  $pk_{A_2} := \mathbf{g}^{\mathbf{a}_2}$ .

**Phase 1:** User  $U_A$  randomly chooses  $r_A, \mathfrak{r}_0 \leftarrow \mathbb{Z}_{\ell_1^{e_1}}$  as two ephemeral randomness. Let  $n_1 \leftarrow g(r_A, \mathbf{a}_1)$ ,  $\mathfrak{r} := G(g(r_A, \mathbf{a}_1))$ . Then  $U_A$  computes  $X_0 := \mathbf{g}^{\mathfrak{r}_0}$ ,  $X := \mathbf{g}^{\mathfrak{r}}$ ,  $x_1 := h((\mathbf{g}^{\mathbf{b}_2})^{\mathfrak{r}}) \oplus n_1$ , and sends  $X_0, X, x_1$  to  $U_B$ .  $U_A$  computes  $K_A := H(n_1, X, x_1)$ .

**Phase 2:** User  $U_B$  randomly chooses  $r_B \leftarrow \mathbb{Z}_{\ell_2^{e_2}}$  as the ephemeral randomness and computes  $m_1 || m_0 \leftarrow g(r_B, \mathbf{b}_2)$ ,  $\eta \leftarrow G(m_1, m_0)$ , and  $Y := \mathbf{g}^\eta$ . On receiving  $(X_0, X, x_1)$  from  $U_A$ ,  $U_B$  computes  $y_1 := h((\mathbf{g}^{\mathbf{a}_1})^\eta) \oplus m_1$ ,  $y_0 := h((\mathbf{g}^{\mathfrak{r}_0})^\eta) \oplus m_0$ ,  $K_B := H(X_0, m_1, m_0, Y, y_1, y_0)$ , and sends  $(Y, y_1, y_0)$  to  $U_A$ .  $U_B$  decrypts  $X, x_1$  to extract  $n'_1$  and  $\mathfrak{r}' \leftarrow G(n'_1)$ . If  $X \neq \mathbf{g}^{\mathfrak{r}'}$ , set  $n'_1 := s_{B_2}$ . Let  $K'_A := H(n'_1, X, x_1)$ . The session key is  $SK := \hat{H}(sid, K'_A, K_B)$  where *sid* is  $(U_A, U_B, pk_{A_1}, pk_{B_2}, X, x_1, X_0, Y, y_1, y_0)$ .

**Phase 3:** On receiving  $(Y, y_1, y_0)$  from  $U_B$ ,  $U_A$  computes  $m'_1 := y_1 \oplus h((\mathfrak{g}^\eta)^{\mathfrak{a}_1})$ ,  $m'_0 := y_0 \oplus h((\mathfrak{g}^\eta)^{\mathfrak{r}_0})$  to extract  $\eta' \leftarrow G(m'_1, m'_0)$ . If  $Y \neq \mathfrak{g}^\eta$ , set  $m'_1 || m'_0 := s_{A1}$ . Let  $K'_B := H(X_0, m'_1, m'_0, Y, y_1, y_0)$ . The session key is  $SK := \hat{H}(sid, K_A, K'_B)$  where  $sid$  is  $(U_A, U_B, pk_{A_1}, pk_{B_2}, X, x_1, X_0, Y, y_1, y_0)$ .

The session state owned by  $U_A$  consists of the ephemeral secret key  $r_A, \mathfrak{r}_0$ , the decapsulated key  $K'_B$  and the encapsulated key  $K_A$ . The session state owned by  $U_B$  consists of the ephemeral secret key  $r_B$  and the encapsulated key  $K_B$ , but not the decapsulated key  $K'_A$ .

**Theorem 2.** *Under the SI-DDH assumption,  $\text{SIAKE}_2$  is  $\text{CK}^+$  secure in the random oracle model. Precisely, if the number of users is  $N$  and there are at most  $l$  sessions between any two users, for any PPT adversary  $\mathcal{A}$  against  $\text{SIAKE}_2$  with  $q$  times of hash oracle queries, there exists  $\mathcal{B}$  s.t.*

$$\text{Adv}_{\text{SIAKE}_2}^{\text{CK}^+}(\mathcal{A}) \leq 1/2 + N^2 \cdot l \cdot q \cdot \left( 4\text{Adv}_{\mathcal{B}}^{\text{sid dh}} + \frac{q+1}{2^n} + \text{negl} \right).$$

Proof sketch: Obviously,  $U_A$  sends  $X_0$  and a OW-CCA secure ciphertext  $X, x_1$  under public key  $pk_{B_2}$  to  $U_B$ .  $U_B$  responds with a [OW-CCA, OW-CPA] secure ciphertext  $Y, y_1, y_0$  under public keys  $pk_{A_1}$  and  $X_0$  to  $U_A$ . We first assume that the AKE adversary only has the capability to Send message and does not query SessionKeyReveal and SessionStateReveal on non-test sessions. Then under the assumption of [OW-CPA, OW-CPA] security,  $\text{SIAKE}_2$  is secure. Take the event  $E_3$  (one of the behaviors presented in Appendix A Table 6) as an example, where the adversary may send  $X_0$  in the test session and he/she knows  $\mathfrak{b}_2$  but not  $\mathfrak{a}_1$  or  $r_B$ . Since the adversary does not know  $\mathfrak{a}_1$  and  $\eta$ , the [OW-CPA, OW-CPA] security guarantees that  $K_B$  encapsulated in  $(Y, y_1, y_0)$  is secure (thus  $SK$  is random assuming  $\hat{H}$  is a random oracle) even the adversary chooses part of the public key  $X_0$ . Note that to simulate the  $\text{CK}^+$  game and reduce the advantage of the AKE adversary to the advantage of solving underlying [OW-CPA, ·] game, the simulator does not hold the static secret key  $\mathfrak{a}_1$  of  $U_A$ . It is safe if the adversary does not make SessionKeyReveal and SessionStateReveal queries. However if the adversary makes SessionKeyReveal queries that involves  $U_A$ , the simulator fails to compute the encapsulated key and session key. Nevertheless, when the underlying KEM is [OW-CCA, OW-CPA] secure, the simulator could query the strong decapsulation oracle to get the encapsulated key and session key, so the reduction works. In other events, the proof proceeds similarly.

*Proof.* We give representative security proof in two cases  $E_5$  and  $E_3$  in Table 2, where one is wPFS and the other is the MEX attack. The other cases can be easily extended or modified from the proof of  $E_3$ , so they are omitted here. Table 3 presents the outline of reduction.

**wPFS  $E_5$ .** The proof of this case proceeds via a sequence of games, i.e. Game 0 to 2. In this case, the test session  $\text{sid}^*$  (with owner as responder or initiator) has a matching session  $\overline{\text{sid}}^*$ . Both static secret keys of the initiator and the responder are leaked to  $\mathcal{A}$ . We denote the event that the AKE adversary  $\mathcal{A}$  outputs  $b'$  such that  $b = b'$  as  $\text{Succ}_i$  in Game  $i$ .

Assumption	2-Key PKE	2-Key KEM	Cases in Table 2
SI-DDH	$[\cdot, \text{OW-CPA}], pk_0 = \mathbf{g}^{r_0}$	$[\cdot, \text{OW-CPA}], pk_0 = \mathbf{g}^{r_0}$	$E_5$
SI-DDH	$[\text{OW-CPA}, \cdot], pk_1 = \mathbf{g}^{a_1}$	$[\text{OW-CCA}, \cdot], pk_1 = \mathbf{g}^{a_1}$	$E_3, E_4, E_6, E_{7-2}, E_{8-1}$
SI-DDH	OW-CPA	OW-CCA, $pk_1 = \mathbf{g}^{b_2}$	$E_1, E_2, E_{7-1}, E_{8-2}$

**Table 3.** The outline of security reduction for SIAKE<sub>2</sub>.

**Game 0:** This is the original CK<sup>+</sup> game in case  $E_5$ . In the test session, the adversary owns all the static secret keys, i.e.  $\mathbf{a}_1, \mathbf{a}_2, \mathbf{b}_1, \mathbf{b}_2$  assuming the test session is between  $U_A$  and  $U_B$ .

**Game 1:** In this game, we change the way to generate  $m_1 || m_0$  in the test session by replacing  $m_1 || m_0 \leftarrow g(r_B, \mathbf{b}_2)$  with  $m_1 || m_0 \leftarrow \{0, 1\}^{2n}$ . Since  $g$  is a random oracle,  $\Pr[\text{Succ}_0] - \Pr[\text{Succ}_1] \leq N^2 \cdot l \cdot \frac{q}{2^n}$ .

**Game 2:** In this game, we change the session key in the test session by replacing  $\hat{H}(\text{sid}, K'_A, K_B)$  with a random bit-string in  $\{0, 1\}^n$ . Obviously,  $\Pr[\text{Succ}_2] = 1/2$ .

We construct an algorithm  $\mathcal{B}$  to solve the  $[\cdot, \text{OW-CPA}]$  security of  $2\text{KEM}_{\text{sidh}}$ , if there exists an algorithm  $\mathcal{A}$  to distinguish Game 1 and Game 2.

On receiving the public key  $pk_0$  from the  $[\cdot, \text{OW-CPA}]$  challenger, to simulate the CK<sup>+</sup> game,  $\mathcal{B}$  randomly chooses two parties  $U_A, U_B$  and the  $i$ -th session as a guess of the test session with success probability  $1/N^2 l$ .  $\mathcal{B}$  computes and sets all the static secrets and public key pairs by himself for all  $N$  users  $U_P$  as both responder and initiator. Particularly,  $\mathcal{B}$  sets the static secret and public key pair  $(pk_{B_2}, sk_{B_2})$  for  $U_B$  as responder, and sets  $pk_{A_1}$  for  $U_A$  as initiator.  $\mathcal{B}$  sends  $pk_{A_1}$  to  $[\cdot, \text{OW-CPA}]$  challenger and receives the challenge ciphertext  $C^*$ . Then  $\mathcal{B}$  simulates all the communications and `SessionStateReveal` and `SessionKeyReveal` as those in Game 1 except the test session. In the test session,  $\mathcal{B}$  sets  $X_0 = pk_0$  and responds  $(Y, y_1, y_0) = C^*$ .

Finally,  $\mathcal{B}$  checks the hash list queried by  $\mathcal{A}$ . If there exists some  $(U_A, U_B, pk_{A_1}, pk_{B_2}, X, x_1, X_0, C^*, K_A, K_B)$  in the list such that  $K_A$  is the key encapsulated in  $(X, x_1)$  (since  $(X, x_1)$  is honestly generated by  $\mathcal{B}$ , it can compute  $K_A$ ),  $\mathcal{B}$  chooses a random one and outputs  $K_B$ , otherwise  $\perp$ . Denote `flag` as the event that  $\mathcal{A}$  explicitly queries  $(U_A, U_B, pk_{A_1}, pk_{B_2}, X, x_1, X_0, C^*, K_A, K_B)$  to the oracle  $\hat{H}$  such that  $K_A$  is the key encapsulated in  $(X, x_1)$  and  $K_B$  is the key encapsulated in  $C^*$ . If `flag` does not happen,  $\mathcal{B}$  perfectly simulates both Game 1 and Game 2. Thus,

$$\Pr[\text{Succ}_1] - \Pr[\text{Succ}_2] \leq \Pr[\text{flag}] \leq N^2 \cdot l \cdot \text{Adv}_{2\text{PKE}_{\text{sidh}}}^{[\cdot, \text{OW-CPA}]}(\mathcal{C}).$$

$$\text{By Lemma 2, } \Pr[\text{Succ}_0] \leq 1/2 + N^2 \cdot l \cdot \left( \frac{q}{2^n} + 2\text{Adv}_{\mathcal{B}}^{\text{sidh}} + 1/2^n + \text{negl} \right).$$

**MEX  $E_3$ .** In this case, the test session  $\text{sid}^*$  with its owner as responder does not have a matching session which means that  $X, x_1, X_0$  is sent by adversary. And the randomness  $r_B$  are leaked to  $\mathcal{A}$ . It is more complicated than  $E_5$ . At first,  $(X, x_1, X_0)$  in the test session is generated by  $\mathcal{A}$  rather than  $\mathcal{B}$ . However,  $(X, x_1)$  is the ciphertext under public key  $pk_{B_2}$ , and the encapsulated key  $K_A$  can be extracted with  $sk_{B_2}$ . Furthermore, the challenge public key that the security relies upon is the static public key, and this will affect the simulation of answering

SessionStateReveal and SessionKeyReveal queries. Fortunately,  $2\text{PKE}_{sidh}$  provides a strong decapsulation oracle to answer those queries.

The proof also proceeds via a sequence of games, i.e., Game 0 to 2. We denote the event that  $\mathcal{A}$  outputs  $b'$  such that  $b = b'$  as  $\text{Succ}_i$  in Game  $i$ .

**Game 0:** This is the original  $\text{CK}^+$  game in case  $E_3$ . In the test session,  $r_B$  is leaked to the adversary assuming the test session is between  $U_A$  and  $U_B$ .

**Game 1:** In this game, we change the way to generate  $m_1||m_0$  in the test session by replacing  $m_1||m_0 \leftarrow g(r_B, \mathbf{b}_2)$  with  $m_1||m_0 \leftarrow \{0, 1\}^{2n}$ . Although  $r_B$  is leaked to  $\mathcal{A}$ , since  $g$  is a random oracle,  $\mathcal{A}$  will not find this change without querying  $g$  with  $r_B, \mathbf{b}_2$ . We denote  $\text{Ask}_g$  as the event  $\mathcal{A}$  queries  $g$  with  $r_B, \mathbf{b}_2$ . If event  $\text{Ask}_g$  happens, we can extract  $\mathbf{b}_2$  and utilize it to solve the underlying SI-DDH problem. Precisely, given  $(\mathbf{g}, \mathbf{g}_1, \mathbf{g}_2, j)$ ,  $\mathcal{B}$  randomly chooses  $U_B$  as a guess of the responder in the test session with success probability  $\frac{1}{2N}$ .  $\mathcal{B}$  sets  $pk_{B_2} := \mathbf{g}_2$ . When event  $\text{Ask}_g$  happens,  $\mathcal{B}$  uses  $\mathbf{b}_2$  to output  $j \stackrel{?}{=} \mathbf{g}_1^{\mathbf{b}_2}$ .

$$\Pr[\text{Succ}_0] - \Pr[\text{Succ}_1] \leq 2N \cdot \text{Adv}_{\mathcal{B}}^{\text{sidh}}.$$

**Game 2:** In this game, we change the session key in the test session by replacing  $\hat{H}(sid, K'_A, K_B)$  with a random bit-string in  $\{0, 1\}^n$ . Obviously,  $\Pr[\text{Succ}_2] = 1/2$ .

We construct an algorithm  $\mathcal{B}$  to solve the  $[\text{OW-CCA}, \cdot]$  security of  $2\text{KEM}_{sidh}$ , if there exists an algorithm  $\mathcal{A}$  to distinguish Game 1 and Game 2.

On receiving the public key  $pk_1$  from the  $[\text{OW-CPA}, \cdot]$  challenger, to simulate the  $\text{CK}^+$  game,  $\mathcal{B}$  randomly chooses two parties  $U_A, U_B$  and the  $i$ -th session as a guess of the test session with success probability  $1/N^2l$ .  $\mathcal{B}$  computes and sets all the static secret and public key pairs on his own for all  $N$  users  $U_P$  as both responder and initiator except the static public key for  $U_A$  as initiator.

- Specifically,  $\mathcal{B}$  sets the static secret and public key pair  $(pk_{A_2}, sk_{A_2})$  that involves  $U_A$  as responder, and sets  $pk_1$  (receiving from the  $[\text{OW-CPA}, \cdot]$  challenger) for  $U_A$  as initiator.
- In the test session, on receiving  $(X, x_1, X_0)$  from  $\mathcal{A}$ ,  $\mathcal{B}$  sends  $pk_0^* = X_0$  to the  $[\text{OW-CCA}, \cdot]$  challenger and receives the challenge ciphertext  $C^*$ . Then  $\mathcal{B}$  returns  $C^*$  to  $\mathcal{A}$  as response.
- $\mathcal{B}$  simulates all the communications and SessionStateReveal and SessionKeyReveal queries as those in Game 1 except that involves  $U_A$  as initiator (since  $\mathcal{B}$  does not know  $sk_{A_1}$ ).
- For those SessionStateReveal and SessionKeyReveal queries involves  $U_A$  as initiator (for example,  $U_A$  honestly sends out  $X', x'_1, X'_0$  and receives  $(Y', y'_1, y'_0)$ ),  $\mathcal{B}$  queries the  $\mathcal{O}$  oracle with  $(X'_0; Y', y'_1, y'_0)$  provided by the  $[\text{OW-CCA}, \cdot]$  challenger to extract the encapsulated key and maintains the consistency of the  $\hat{H}$  list with SessionStateReveal and SessionKeyReveal queries.

Finally,  $\mathcal{B}$  checks the hash list queried by  $\mathcal{A}$ . If there exists some  $(U_A, U_B, pk_{A_1}, pk_{B_2}, X, x_1, X_0, C^*, K_A, K_B)$  in the list such that  $K_A$  is the key encapsulated in  $(X, x_1)$  (since  $(X, x_1)$  is honestly generated by  $\mathcal{B}$ , it can compute  $K_A$ ),  $\mathcal{B}$  chooses a random one and outputs  $K_B$ , otherwise  $\perp$ . Denote  $\text{flag}$  as the event that  $\mathcal{A}$  explicitly queries  $(U_A, U_B, pk_{A_1}, pk_{B_2}, X, x_1, X_0, C^*, K_A, K_B)$  to the oracle  $\hat{H}$

such that  $K_A$  is the key encapsulated in  $(X, x_1)$  and  $K_B$  is the key encapsulated in  $C^*$ . If **flag** does not happen,  $\mathcal{B}$  perfectly simulates both Game 1 and Game 2. Thus,

$$\Pr[\text{Succ}_1] - \Pr[\text{Succ}_2] \leq \Pr[\text{flag}] \leq N^2 \cdot l \cdot \text{Adv}_{2\text{KEM}_{\text{sidh}}}^{\text{OW-CCA}, \cdot}(\mathcal{C}).$$

By Theorem 1, to sum up,

$$\Pr[\text{Succ}_0] \leq 1/2 + N^2 \cdot l \cdot q \cdot \left( 4\text{Adv}_{\mathcal{B}}^{\text{sidh}} + 1/2^n + \text{negl} \right).$$

□

## 5 Three-pass SIAKE

We first enhance the SI-DDH assumption to 1-Oracle SI-DH assumption, and analyze its reliability. Based on this assumption, we propose the three-pass SIAKE<sub>3</sub>.

### 5.1 1-Oracle SI-DH and Implied 2-key KEM

The 1-Oracle SI-DH assumption is inspired by the Oracle Diffie-Hellman assumption over classical group given by Abdalla, Bellare and Rogaway [1] for analyzing DHIES. Let  $G := \langle g \rangle$  and  $|G| = p$  be a prime. The Oracle Diffie-Hellman assumption states that, given  $(g, g^a, g^b, h)$ , it is difficult to decide whether  $h = H(g^{ab})$  or not (where  $H$  is a hash function), even the solver could make polynomial queries to an oracle  $H_B(\cdot)$  which will return  $H(v^b)$  with  $v \in G$  satisfying  $v \neq g^a$ . Under the Oracle Diffie-Hellman assumption, the DHIES scheme is chosen ciphertext secure [1].

However, the Oracle Diffie-Hellman assumption can not be directly extended in the supersingular isogeny setting. As we have presented several times before, the adaptive attack [17] would allow extraction of every bit of  $b$  with polynomial queries to  $H_B(\cdot)$  with specified points, implying the analogue of Oracle Diffie-Hellman problem in the supersingular isogeny setting could be solved. Moreover, in the classical group, if  $v \neq g^a$ , then  $v^b \neq (g^a)^b$ . However, in the supersingular isogeny setting, even if  $v \neq g^a \in \text{SSEC}_A$ , it is possible that  $v^b$  is equal to  $(g^a)^b$ .

Fortunately, only one query to  $H_B(\cdot)$  with  $v \neq g^a$  is needed for our purpose and the adaptive attack does not work. Furthermore, when  $H_B(v) = H(v, v^b)$ , even if  $v \neq g^a$ , the case  $H(v, v^b) = H(g^a, (g^a)^b)$  occurs with negligible probability.

**Definition 4 (1-Oracle SI-DH Assumption).** Let  $H : \{0, 1\}^* \rightarrow \{0, 1\}^n$  be a hash function. Let  $\mathfrak{e}$  and  $\mathfrak{g}$  be public parameters as defined in SI-DDH assumption. Let  $D_0$  and  $D_1$  be two distributions:

$$\begin{aligned} D_1 &:= \{ \mathfrak{e}, \mathfrak{g}, \mathfrak{g}^a, \mathfrak{g}^b, H(\mathfrak{g}^a, (\mathfrak{g}^a)^b) \mid \mathfrak{a} \leftarrow \mathbb{Z}_{\ell_s^{e_s}}, \mathfrak{b} \leftarrow \mathbb{Z}_{\ell_t^{e_t}} \} \\ D_0 &:= \{ \mathfrak{e}, \mathfrak{g}, \mathfrak{g}^a, \mathfrak{g}^b, h \mid \mathfrak{a} \leftarrow \mathbb{Z}_{\ell_s^{e_s}}, \mathfrak{b} \leftarrow \mathbb{Z}_{\ell_t^{e_t}}, h \leftarrow \{0, 1\}^n \} \end{aligned}$$

The 1-Oracle SI-DH problem is, given a random sample from  $D_b$  depending on  $b \leftarrow \{0, 1\}$ , and a one-time oracle  $H_B$ , guessing  $b$ . The one-time oracle  $H_B$  can

be queried only one time with  $\eta \in SSEC_A$  and  $\eta \neq \mathfrak{g}^a$ , and it will return  $H(\eta, \eta^b)$ . The advantage of  $\mathcal{A}$  to solve the 1-Oracle SI-DH problem is

$$Adv_{\mathcal{A}}^{1osidh} = Pr[b' = b | \mathcal{A}^{H_B(\cdot)}(\mathfrak{d}_b \leftarrow D_b) = b', b \leftarrow \{0, 1\}] - 1/2.$$

The 1-Oracle SI-DH assumption states that for any PPT algorithm  $\mathcal{A}$ ,  $Adv_{\mathcal{A}}^{1osidh}$  is negligible.

We emphasize that the adversary is allowed to query the hashed SIDH oracle  $H_B$  only once with  $\eta \neq \mathfrak{g}^a$ . If there are polynomial queries, the 1-Oracle SI-DH problem can be solved by the adaptive attack in [17]. Please also notice that the hash function involves  $\mathfrak{g}^a$  or  $\eta$  as input besides the  $j$ -invariant. Otherwise the 1-Oracle SI-DH problem is easy. Let  $\mathfrak{g}^a = (E_A, \phi_A(P_t), \phi_A(Q_t))$ . Since  $\langle \phi_A(P_s) + [y]\phi_A(Q_s) \rangle = \langle [u]\phi_A(P_s) + [y][u]\phi_A(Q_s) \rangle$  for any integer  $1 \leq u \leq \ell_s^{e_s}$  and coprime to  $\ell_s$ , the attacker sets  $E_Y = E_A$ ,  $R = [u]\phi_A(P_s)$ ,  $S = [u]\phi_A(Q_s)$  and  $\eta = (Y, R, S)$ . Then  $(\mathfrak{g}^a)^b$  and  $\eta^b$  will produce the same  $j$ -invariant. However, when taking  $\mathfrak{g}^a$  or  $\eta$  as input of  $H$ , any query with  $\eta \neq \mathfrak{g}^a$  to  $H_B$  will get a completely different value.

1-Gap SI-DH problem is similar to the SI-CDH problem but the adversary is given access to a highly restricted SI-DDH oracle.

**Definition 5 (1-Gap SI-DH Assmption).** Let  $\mathfrak{e}$  and  $\mathfrak{g}$  be public parameters. The 1-Gap SI-DH problem is that, given  $\mathfrak{g}^a, \mathfrak{g}^b$  (where  $\mathfrak{a} \leftarrow \mathbb{Z}_{\ell_s^{e_s}}, \mathfrak{b} \leftarrow \mathbb{Z}_{\ell_t^{e_t}}$ ), and an oracle  $\mathcal{O}_{sidh}(\eta, \cdot)$ , compute the  $j$ -invariant  $(\mathfrak{g}^a)^b = (\mathfrak{g}^b)^a$ . Here,  $\eta \in SSEC_A$  is chosen by the adversary  $\mathcal{A}$  at any time before its first queries to  $\mathcal{O}_{sidh}(\eta, \cdot)$ .  $\mathcal{O}_{sidh}(\eta, j)$  will return 1 if  $j = \eta^b$ , and 0 otherwise. For any PPT algorithm  $\mathcal{A}$ , we define the advantage of solving 1-Gap SI-DH problem as

$$Adv_{\mathcal{A}}^{1gsidh} = Pr[j' = (\mathfrak{g}^a)^b | \mathcal{A}^{\mathcal{O}_{sidh}(\eta, \cdot)}(\mathfrak{g}, \mathfrak{e}, \mathfrak{g}^a, \mathfrak{g}^b) \rightarrow (\eta, j')].$$

The 1-Gap SI-DH assumption states: for any PPT algorithm  $\mathcal{A}$ , the advantage of solving 1-Gap SI-DH problem is negligible.

We emphasize that if the adversary is allowed to query  $\mathcal{O}_{sidh}(\cdot, \cdot)$  with unlimited numbers of  $\eta$ , 1-Gap SI-DH problem can be solved using the adaptive attack in [17]. However, here  $\mathcal{O}_{sidh}(\cdot, \cdot)$  oracle only allows to be queried once with  $\eta$  of adversary's choice.

**Discussion.** These two assumptions are “non-standard” for supersingular isogeny. The adaptive attack [17] and its extension can not easily break these new assumptions. We encourage more works on the analysis of the hardness of these two problems.

The following theorem shows that the 1-Gap SI-DH assumption implies the 1-Oracle SI-DH assumption when the hash function  $H$  is modeled as a random oracle.

**Theorem 3.** For any algorithm  $\mathcal{A}$  against the 1-Oracle SI-DH problem there exists an algorithm  $\mathcal{B}$  against the 1-Gap SI-DH problem such that

$$Adv_{\mathcal{A}, H}^{1osidh}(n) \leq q_H \cdot Adv_{\mathcal{B}}^{1gsidh}(n),$$

where  $q_H$  is the number of times to query  $\mathcal{O}_{sidh}(\eta, \cdot)$ .

*Proof.* Let  $\mathcal{A}$  be any algorithm solving the 1-Oracle SI-DH problem. We construct an algorithms  $\mathcal{B}$  to solve the 1-Gap SI-DH problem using  $\mathcal{A}$  as a subroutine in Figure 8. The challenge is how to maintain the hash list so as to keep the consistency with the one-time Oracle  $H_B$ . Actually, the limited oracle  $\mathcal{O}_{\text{sidh}}(\cdot, \cdot)$  would help  $\mathcal{B}$  to fix it.

<b>Algorithm</b> $\mathcal{B}^{\mathcal{O}_{\text{sidh}}(\cdot, \cdot)}(\mathfrak{c}, \mathfrak{g}, \mathfrak{g}^a, \mathfrak{g}^b)$	
01 $h_0, h_1 \leftarrow \{0, 1\}^n$	One time $H_B(\eta)$
02 $b \leftarrow \{0, 1\}$	01 Choose $\eta$ as the base of $\mathcal{O}_{\text{sidh}}$
03 Run $\mathcal{A}^{H_B(\cdot), H}(\mathfrak{g}, \mathfrak{g}^a, \mathfrak{g}^b, h_b)$	02 if $\exists(\eta, j', h') \in L_H \wedge \mathcal{O}_{\text{sidh}}(\eta, j') = 1$
04 a. For one-time query $H_B$	03 return $h'$
05 do as one-time $H_B$	04 else $h'' \leftarrow \{0, 1\}^n, L_H = L_H \cup \{\eta, j', h''\}$
06 b. For the $H$ -query	05 return $h''$
07 do as $H(x, j')$	$H(x, j')$
08 c. Let $b'$ be the output of $\mathcal{A}$	01 if $\exists(x, j', h') \in L_H$ return $h'$
09 return $(\cdot, j, \cdot) \leftarrow L_H$	02 otherwise $h \leftarrow \{0, 1\}^n, L_H = L_H \cup \{(x, j', h)\}$
10 return $j$	03 return $h$

**Fig. 8.** Algorithm  $\mathcal{B}$  for attacking the 1-Gap SI-DH problem.

Note that in Figure 8, if  $H_B(\eta)$  is asked at first and returns a random  $h$ , then when  $(\eta, j')$  is queried to  $H$  such that  $\mathcal{O}_{\text{sidh}}(\eta, j') = 1$ , it will return  $h$ . If  $H(\eta, j')$  is asked at first and returns a random  $h$ , then when  $\eta$  is asked to  $H_B$  such that  $\mathcal{O}_{\text{sidh}}(\eta, j') = 1$ , it will return that  $h$ .

Let  $\text{Ask}$  be the event that  $(\mathfrak{g}^a, (\mathfrak{g}^a)^b)$  is queried to  $H$  and  $\overline{\text{Ask}}$  be the complement of  $\text{Ask}$ . If  $\text{Ask}$  does not happen, there is no way to tell whether  $h_b$  is equal to  $H(\mathfrak{g}^a, (\mathfrak{g}^a)^b)$  or not. Thus we have that

$$\begin{aligned}
\text{Adv}_{\mathcal{A}, H}^{\text{1osidh}} &= \Pr[\mathcal{A}^{H_B(\cdot)}(\mathfrak{b} \leftarrow D_b) = b] - 1/2 \\
&= \Pr[\mathcal{A}^{H_B(\cdot)}(\mathfrak{b} \leftarrow D_b) = b \wedge \text{Ask}] + \Pr[\mathcal{A}^{H_B(\cdot)}(\mathfrak{b} \leftarrow D_b) = b \wedge \overline{\text{Ask}}] - 1/2 \\
&= \Pr[\mathcal{A}^{H_B(\cdot)}(\mathfrak{b} \leftarrow D_b) = b \wedge \text{Ask}] \\
&\leq \Pr[\text{Ask}] \leq q_H \cdot \text{Adv}_{\mathcal{B}}^{\text{1gsidh}}.
\end{aligned}$$

□

We now modify the  $2\text{PKE}_{\text{sidh}}$  and denote the new scheme as  $2\text{PKE}_{\text{1osidh}}$ . The key generation algorithms are the same. In the encryption algorithm,  $h((\mathfrak{g}^b)^{a_1})$  is replaced by  $h(\mathfrak{g}^b, (\mathfrak{g}^b)^{a_1})$  and  $h((\mathfrak{g}^b)^{a_0})$  is replaced by  $h(\mathfrak{g}^b, (\mathfrak{g}^b)^{a_0})$ . Thus the ciphertext is  $c := (\mathfrak{g}^b, h(\mathfrak{g}^b, (\mathfrak{g}^b)^{a_1}) \oplus m_1, h(\mathfrak{g}^b, (\mathfrak{g}^b)^{a_0}) \oplus m_0)$ .

**Lemma 3.** *The following holds.*

- Under the 1-Oracle SI-DH assumption, the scheme  $2\text{PKE}_{\text{1osidh}}$  is  $[\text{OW-CPA}, \cdot]$  secure even  $H(pk_0^*, pk_0^{*b})$  is given to the adversary besides the challenge ciphertext  $c^* = (c_1^* = \mathfrak{g}^b, c_1, c_2)$ .

- If the  $[\text{OW-CPA}, \cdot]$  game is changed as that  $pk_0^*$  is generated by the challenger and the corresponding  $sk_0^*$  is leaked to the adversary, then under the SI-DDH assumption,  $2PKE_{1osidh}$  satisfies this  $[\text{OW-CPA}, \cdot]$  security even  $H(pk_0^*, pk_0^{*b})$  is given to the adversary besides the challenge ciphertext  $c^* = (c_1^* = \mathbf{g}^b, c_1, c_2)$ .
- Under the SI-DDH assumption, the scheme  $2PKE_{1osidh}$  is  $[\cdot, \text{OW-CPA}]$  secure.

*Proof.* The  $[\cdot, \text{OW-CPA}]$  security is the same with that in Lemma 2. We reduce the  $[\text{OW-CPA}, \cdot]$  security with leakage to the underlying 1-Oracle SI-DH assumption.

**Game 0:** This is the original  $[\text{OW-CPA}, \cdot]$  challenge game in Fig. 3. We denote the event that the adversary wins the games as  $\text{Succ}_0$ .

**Game 1:** In this game, we modify the computation of challenge ciphertext. Specifically,  $h(\mathbf{g}^b, (\mathbf{g}^b)^{a_1})$  is replaced by a random bit  $h \leftarrow \{0, 1\}^n$ . We construct an algorithm  $\mathcal{B}$  to solve the 1-Oracle SI-DH problem given an instance  $(\mathbf{g}, \mathbf{g}_1, \mathbf{g}_2, h)$ , and a one-time oracle  $\mathcal{H}_B(\cdot)$ , if there exists an algorithm  $\mathcal{A}$  to distinguish Game 0 and Game 1.

---

```

 $\mathcal{B}^{\mathcal{H}_B(\cdot)}(\mathbf{c}, \mathbf{g}, \mathbf{g}_1, \mathbf{g}_2 = \mathbf{g}^b, h)$ 
01  $pk_1 \leftarrow \mathbf{g}_1$ 
02  $pk_0^*, \text{state} \leftarrow \mathcal{A}(pk_1)$ 
03  $m_1 \leftarrow \{0, 1\}^n, m_0 \leftarrow \{0, 1\}^n$ 
04 Query  $\mathcal{H}_B$  with  $pk_0^*$  and get  $pk_0^{*b}$ 
04  $c_1^* = \mathbf{g}_2, c_2^* = h \oplus m_1, c_3^* = h(pk_0^*, pk_0^{*b}) \oplus m_0$ 
05  $c^* = (c_1^*, c_2^*, c_3^*)$ 
06  $m'_1 || m'_0 \leftarrow \mathcal{A}(\text{state}, C^*)$ 
07 If  $m'_1 = m_1, b' = 1$ , else  $b' \leftarrow \{0, 1\}$ .

```

---

If  $(\mathbf{g}, \mathbf{g}_1, \mathbf{g}_2, h)$  is a 1-Oracle SI-DH tuple,  $\mathcal{B}$  perfectly simulates Game 0, else  $\mathcal{B}$  perfectly simulates Game 1. In the 1-Oracle SI-DH challenge, we have

$$\begin{aligned}
\text{Adv}_{\mathcal{B}}^{1osidh} &= \Pr[b = b'] - 1/2 \\
&= 1/2(\Pr[b' = 1|b = 1] - \Pr[b' = 1|b = 0]) \\
&= 1/2(\Pr[b' = 1|\text{Game 0}] - \Pr[b' = 1|\text{Game 1}]) \\
&= 1/2(\Pr[\text{Succ}_0] - \Pr[\text{Succ}_1]).
\end{aligned}$$

Note that in this game, the  $[\text{OW-CPA}, \cdot]$  advantage is less than  $1/2^n$ . To Sum up, we have that,  $\Pr[\text{Succ}_0] \leq 2\text{Adv}_{\mathcal{B}}^{1osidh} + 1/2^n$ .  $\square$

Similarly, we make the same modification to the  $2KEM_{sidh}$  and denote the new scheme as  $2KEM_{1osidh}$ .

**Theorem 4.** *The following holds in the random oracle model.*

- Under the 1-Oracle SI-DH assumption, the scheme  $2KEM_{1osidh}$  is [OW-CCA, ·] secure in the random oracle model, even  $h(pk_0^*, pk_0^{*b})$  is given to the adversary besides the challenge ciphertext  $c^* = (c_1^* = g^b, c_1, c_2)$ .
- If the [OW-CCA, ·] game is changed as that  $pk_0^*$  is generated by challenger and the corresponding  $sk_0^*$  is leaked to the adversary, then under the SI-DDH assumption,  $2KEM_{1osidh}$  satisfies this [OW-CPA, ·] security even  $H(pk_0^*, pk_0^{*b})$  is given to the adversary besides the challenge ciphertext  $c^* = (c_1^* = g^b, c_1, c_2)$ .
- Under the SI-DDH assumption, the scheme  $2KEM_{1osidh}$  is [·, OW-CPA] secure.

## 5.2 A Three-pass AKE based on 1-Oracle SI-DH Assumption

The three-pass AKE  $SIKE_3$  is shown in Fig. 9. The public parameters and register are the same with those for  $SIKE_2$ .

**Phase 1:** User  $U_A$  chooses ephemeral randomness  $r_A$ . Let  $n_1 || n_0 \leftarrow g(r_A, \mathbf{a}_1)$  and  $\mathfrak{r} \leftarrow G(n_1, n_0)$ . Then  $U_A$  computes  $X := g^{\mathfrak{r}}$ ,  $x_1 := h(g^{b_2}, (g^{b_2})^{\mathfrak{r}}) \oplus n_1$ , and sends  $X, x_1$  to  $U_B$ .

**Phase 2:** User  $U_B$  chooses ephemeral randomness  $r_B \leftarrow \mathbb{Z}_{\ell^2}$ , computes  $m_1 || m_0 \leftarrow g(r_B, \mathbf{b}_2)$ ,  $\eta \leftarrow G(m_1, m_0)$ , and  $Y := g^\eta$ . On receiving  $(X, x_1, X_0)$  from  $U_A$ , if  $X := pk_{B_2}$ , aborts, else  $U_B$  computes  $y_1 := h(g^{a_1}, (g^{a_1})^\eta) \oplus m_1$ ,  $y_0 := h(X, (g^{\mathfrak{r}})^\eta) \oplus m_0$ ,  $K_B := H(X, m_1, m_0, Y, y_1, y_0)$ , and sends  $(Y, y_1, y_0)$  to  $U_A$ .

**Phase 3:** On receiving  $(Y, y_1, y_0)$  from  $U_B$ , if  $Y := pk_{A_1}$ , aborts, else  $U_A$  decrypts  $Y, y_1, y_0$  to extract  $m'_1 || m'_0$  and  $\eta' \leftarrow G(m'_1, m'_0)$ . If  $Y \neq g^\eta$ , then  $m'_1 || m'_0 := s_{A1}$ .  $U_A$  computes  $K'_B := H(X, m'_1, m'_0, Y, y_1, y_0)$  and the session key as  $SK := \hat{H}(sid, K_A, K'_B)$ , where  $sid$  is  $(U_A, U_B, pk_{A_1}, pk_{B_2}, X, x_1, x_0, Y, y_1, y_0)$ .

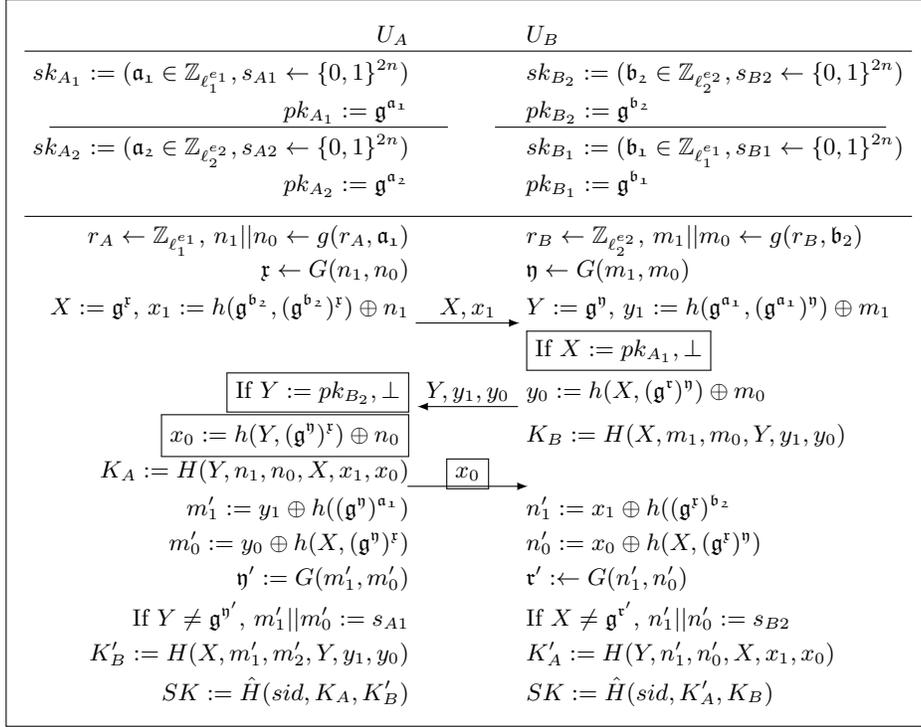
**Phase 4:** If  $X := pk_{B_2}$ , then aborts, else  $U_B$  decrypts  $X, x_1, x_0$  to extract  $n'_1, n'_0$  and  $\mathfrak{r}' \leftarrow G(n'_1, n'_0)$ . If  $X \neq g^{\mathfrak{r}'}$ , then  $n'_1 || n'_0 := s_{B2}$ . Let  $K'_A := H(Y, n'_1, n'_0, X, x_1, x_0)$ . The session key is computed as  $SK := \hat{H}(sid, K'_A, K_B)$  where  $sid$  is  $(U_A, U_B, pk_{A_1}, pk_{B_2}, X, x_1, Y, y_1, y_0, x_0)$ .

The session state of  $U_A$  consists of  $r_A, K'_B$  and  $K_A$ . The session state of  $U_B$  consists of  $r_B, K_B$  and  $K'_A$ .

**Theorem 5.** *Under the 1-Oracle SI-DH assumption,  $SIKE_3$  is  $CK^+$  secure in the random oracle model. Precisely, if the number of users is  $N$  and there are at most  $l$  sessions between any two users, for any PPT adversary  $\mathcal{A}$  against  $SIKE_3$  with  $q$  times of hash oracle queries, there exists  $\mathcal{B}$  s.t.*

$$Adv_{SIKE_3}^{CK^+}(\mathcal{A}) \leq 1/2 + N^2 \cdot l \cdot q \cdot \left( 4Adv_{\mathcal{B}}^{1osidh} + \frac{q+1}{2^n} + negl \right).$$

Please refer full paper [33] for the concrete proof. We only give the proof sketch here: Obviously,  $U_A$  sends [OW-CCA, OW-CPA] secure  $X, x_1, x_0$  under public keys  $pk_{B_2}$  and  $Y$  to  $U_B$ .  $U_B$  responds with [OW-CCA, OW-CPA] secure ciphertexts  $Y, y_1, y_0$  under public keys  $pk_{A_1}$  and  $X_0$  to  $U_A$ . The proof of wPFS security is



**Fig. 9.** A Compact 3-pass AKE  $\text{SIAKE}_3$  based on SIDH. Here  $sid$  is  $(U_A, U_B, pk_{A_1}, pk_{B_2}, X, x_1, x_0, Y, y_1, y_0)$ . The boxed arguments are the main differences with  $\text{SIAKE}_2$ . Besides, the input of  $h$  includes the first part of the public key.

exactly the same as that of  $\text{SIAKE}_2$ , but different for other security cases. The main observation is the same: since the underlying KEM is  $[\text{OW-CCA}, \cdot]$  secure, the simulator could query the strong decapsulation oracle to get the encapsulated key and session key and simulate the `SessionKeyReveal` and `SessionStateReveal`. However, this is not sufficient. Take  $E_3$  for example, given  $Y^*, y_1^*, y_0^*$  as the challenge ciphertext, the simulator obviously does not know the randomness of  $Y^*$ , but in the test session  $Y^*$  is the public key of  $(X, x_1, x_0)$ . Fortunately, the underlying 1-Oracle SI-DH assumption provides this capability to encapsulate one ciphertext.

## 6 Implementation and Comparison

We implement  $\text{SIAKE}_2$  and  $\text{SIAKE}_3$ , and compare their performance with [13], [2,26] and the lattice-based Kyber-AKE [3].

We adopt the curve `SIKEp751` in `SIKE` [20] that is proceeding the second round of NIST's post-quantum standardization. The performance is benchmarked on an Intel(R) Core i7-6567U CPU @3.30GHz processor supporting the

Skylake micro-architecture. Kyber-AKE is an AKE based on lattice and others are all considered in the SIDH setting. The comparison of bandwidth is shown in Table 4. The comparison of efficiency is shown in Table 5.

Scheme	$A \rightarrow B$	$B \rightarrow A$	$A \rightarrow B$	total(byte)
Kyber-AKE [3]	2272	2368	-	4640
FSXY [13]	1160	1160	-	2320
BCNP [2,26]	1160	1160	-	2320
SIAKE <sub>2</sub>	1160	628	-	1788
SIAKE <sub>3</sub>	596	628	32	1176

**Table 4.** Comparison of message sizes. “-” stands for no messages to be transmitted. The message sizes are counted in byte.

Scheme	$A(\text{initial})$	$B$	$A(\text{end})$	$B(\text{end})$	total
FSXY [13]	6,238	14,779	10,124	-	31,141
BCNP-Lon [2]	11,146	20,092	9,563	-	40,801
SIAKE <sub>2</sub>	6,828	13,917	6,641	-	27,386
SIAKE <sub>3</sub>	5,966	4,429	4,922	9,575	24,892

**Table 5.** Comparison of cycle counts. Cycle counts are rounded to  $10^6$  cycles by taking the average of 1,000 trials.

## 7 Conclusion and Open Problem

We propose two AKEs based on supersingular isogeny assumptions. Both of them achieve  $CK^+$  security and support arbitrary registration in the classical random oracle model. However, to fully explain their quantum-resistance, their security in the quantum random oracle model should be analyzed. We leave it as an open problem and future work.

### Acknowledgements.

Haiyang Xue is supported by the National Natural Science Foundation of China (No. 61602473, No. 61672019), and the National Cryptography Development Fund MMJJ20170116. Xiu Xu is supported by the National Natural Science Foundation of China (No.61872442). Man Ho Au is supported by the Research Grant Council of Hong Kong (Grant No. 25206317). Song Tian is supported by the National Natural Science Foundation of China (No. 61802401).

## References

1. Abdalla, M., Bellare, M., Rogaway, P.: The oracle Diffie-Hellman assumptions and an analysis of DHIES. In: Naccache D. (eds) CT-RSA 2001. LNCS, vol 2020, pp. 143-158. Springer, Heidelberg (2001).
2. Boyd, C., Cliff, Y., Nieto, J. M. G., Paterson, K. G.: Efficient One-Round Key Exchange in the Standard Model. In: Mu Y., Susilo W., Seberry J. (eds) ACISP 2008. LNCS, vol 5107, pp 69-83. Springer, Heidelberg (2008).
3. Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Stehlé D.: CRYSTALS - Kyber: a CCA-secure Module-lattice-based KEM. In 2018 IEEE Symposium on Security and Privacy, pp. 353-367.
4. Bellare, M., Rogaway, P.: Entity authentication and key distribution. In: Stinson D.R. (eds) CRYPTO 1993. LNCS, vol 773, pp. 232-249. Springer, Heidelberg.
5. Costello, C., Jao, D., Longa, P., Naehrig, M., Renes, J., Urbanik, D.: Efficient compression of SIDH public keys. In: Coron JS., Nielsen J. (eds) EUROCRYPT 2017. LNCS, vol 10210, pp. 679-706. Springer, Cham (2017).
6. Canetti, R., Krawczyk, H.: Analysis of key-exchange protocols and their use for building secure channels. In: Pfitzmann B. (eds) EUROCRYPT 2001. LNCS, vol 2045, PP.453-474. Springer, Heidelberg (2001).
7. Costello, C., Longa, P., Naehrig, M.: Efficient algorithms for supersingular isogeny Diffie-Hellman. In: Robshaw M., Katz J. (eds) CRYPTO 2016. LNCS, vol 9814, pp. 572-601. Springer, Heidelberg (2016).
8. De Feo, L., Jao, D., Plût, J.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3), 209-247 (2014).
9. Eisentrger, K., Hallgren, S., Lauter, K., Morrison, T., Petit, C.: Supersingular isogeny graphs and endomorphism rings: reductions and solutions. In: Nielsen, J., Rijmen, V. (eds) EUROCRYPT 2018. LNCS, vol 10822, pp 329-368. Springer, Cham (2018).
10. Faz-Hernández, A., López, J., Ochoa-Jimenez, E., Rodríguez-Henríquez, F.: A faster software implementation of the supersingular isogeny Diffie-Hellman key exchange protocol. *IEEE Transactions on Computers*, 67(11), 1622-1636 (2018).
11. Fujisaki, E., Okamoto, T. : Secure integration of asymmetric and symmetric encryption schemes. In: Wiener M. (eds) CRYPTO 1999. LNCS, vol 1666, pp. 537-554. Springer, Heidelberg (1999).
12. Fujioka, A., Suzuki, K., Xagawa, K., Yoneyama, K.: Strongly secure authenticated key exchange from factoring, codes, and lattices. In: Fischlin M., Buchmann J., Manulis M. (eds) PKC 2012. LNCS, vol 7293, pp. 467-484. Springer, Heidelberg (2012).
13. Fujioka, A., Suzuki, K., Xagawa, K., Yoneyama, K.: Practical and post-quantum authenticated key exchange from one-way secure key encapsulation mechanism. In *AsiaCCS 2013*, pp. 83-94.
14. Fujioka, A., Takashima, K., Terada, S., Yoneyama, K.: Supersingular Isogeny Diffie-Hellman Authenticated Key Exchange. In: Lee K. (eds) ICISC 2018. LNCS, vol 11396, pp. 177-195. Springer, Cham (2018).
15. Galbraith, S. D.: Authenticated key exchange for SIDH. *IACR Cryptology ePrint Archive 2018/266*.
16. Galbraith, S. D., Petit, C., Silva, J.: Identification protocols and signature schemes based on supersingular isogeny problems. In: Takagi T., Peyrin T. (eds) ASIACRYPT 2017. LNCS, vol 10624, pp. 3-33. Springer, Cham (2017).

17. Galbraith, S. D., Petit, C., Shani, B., Ti, Y. B.: On the security of supersingular isogeny cryptosystems. In: Cheon J., Takagi T. (eds) ASIACRYPT 2016. LNCS, vol 10031, pp. 63-91. Springer, Heidelberg (2016).
18. Guilhem, C. D. S., Smart, N. P., Warinschi, B.: Generic Forward-Secure Key Agreement Without Signatures. In: Nguyen P., Zhou J. (eds) ISC 2017. LNCS, vol 10599, pp. 114-133. Springer, Cham (2017).
19. Galbraith, S. D., Vercauteren, F.: Computational problems in supersingular elliptic curve isogenies. IACR Cryptology ePrint Archive 2017/774.
20. Jao, D., Azarderakhsh, R., Campagna, M., et al.: Supersingular Isogeny Key Encapsulation. <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions>.
21. Jeong, I. R., Katz, J., Lee, D. H.: One-round Protocols for Two-Party Authenticated Key Exchange. In: Jakobsson M., Yung M., Zhou J. (eds) ACNS 2004. LNCS, vol 3089, pp. 220-232. Springer, Heidelberg (2004).
22. Krawczyk, H.: HMQV: A high-performance secure Diffie-Hellman protocol. In: Shoup V. (eds) CRYPTO 2005. LNCS, vol 3621, pp. 546-566. Springer, Heidelberg (2005).
23. Koziel, B., Azarderakhsh, R., Mozaffari-Kermani, M.: A High-Performance and Scalable Hardware Architecture for Isogeny-Based Cryptography. *IEEE Transactions on Computers*, Volume 67, pp.1594-1609 (2018).
24. Kirkwood, D., Lackey, B. C., McVey, J., Motley, M., Solinas, J. A., Tuller, D.: Failure is not an option: Standardization issues for post-quantum key agreement. In *Workshop on Cybersecurity in a Post-Quantum World* (2015).
25. LeGrow, J.: Post-Quantum Security of Authenticated Key Establishment Protocols. Master's thesis, University of Waterloo (2016).
26. Longa, P.: A Note on Post-Quantum Authenticated Key Exchange from Supersingular Isogenies. IACR Cryptology ePrint Archive 2018/267.
27. LaMacchia, B., Lauter, K., Mityagin, A.: Stronger security of authenticated key exchange. In: Susilo W., Liu J.K., Mu Y. (eds) *ProvSec 2007*. LNCS, vol 4784, pp. 1-16. Springer, Heidelberg (2007).
28. Menezes, A., Qu, M., Vanstone, S.: Some new key agreement protocols providing mutual implicit authentication. *Selected Areas in Cryptography* (1995).
29. Matsumoto, T., Takashima, Y., Imai, H.: On seeking smart public-key-distribution systems. *IEICE TRANSACTIONS* (1976-1990), 69(2), 99-106 (1986).
30. Okamoto, T.: Authenticated key exchange and key encapsulation in the standard model. In: Kurosawa K. (eds) ASIACRYPT 2007. LNCS, vol 4833, pp. 474-484. Springer, Heidelberg (2007).
31. Sun, X., Tian, H., Wang, Y.: Toward quantum-resistant strong designated verifier signature from isogenies. In *INCoS 2012*, pp. 292-296.
32. Urbanik, D., Jao, D.: SoK: The problem landscape of SIDH. IACR Cryptology ePrint Archive 2018/336.
33. Xu, X., Xue, H., Wang, K., Liang, B., Au, H., Tian, S.: Strongly Secure Authenticated Key Exchange from Supersingular Isogenies, IACR Cryptology ePrint Archive 2018/760.
34. Xue, H., Lu, X., Li, B., Liang, B., He, J.: Understanding and Constructing AKE via Double-Key Key Encapsulation Mechanism. In: Peyrin T., Galbraith S. (eds) ASIACRYPT 2018. LNCS, vol 11273, pp. 158-189. Springer, Cham (2018).
35. Yoo, Y., Azarderakhsh, R., Jalali, A., Jao, D., Soukharev, V.: A post-quantum digital signature scheme based on supersingular isogenies. In: Kiayias A. (eds) *FC 2017*. LNCS, vol 10322, pp. 163-181. Springer, Cham (2017).