# Efficient Asymmetric PAKE Compiler from KEM and AE

You Lyu<sup>1,2</sup>, Shengli Liu<sup>1,2</sup>, shengli Liu<sup>1,2</sup>, and Shuai Han<sup>2,3</sup>

 <sup>1</sup> Department of Computer Science and Engineering Shanghai Jiao Tong University, Shanghai 200240, China
 <sup>2</sup> State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China
 <sup>3</sup> School of Cyber Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China {vergil,slliu,dalen17}@sjtu.edu.cn

Abstract. Password Authenticated Key Exchange (PAKE) allows two parties to establish a secure session key with a shared low-entropy password pw. Asymmetric PAKE (aPAKE) extends PAKE in the clientserver setting, and the server only stores a password file instead of the plain password so as to provide additional security guarantee when the server is compromised.

In this paper, we propose a novel generic compiler from PAKE to aPAKE in the Universal Composable (UC) framework by making use of Key Encapsulation Mechanism (KEM) and Authenticated Encryption (AE).

- Our compiler admits efficient instantiations from lattice to yield lattice-based post-quantum secure aPAKE protocols. When instantiated with Kyber (the standardized KEM algorithm by the NIST), the performances of our compiler outperform other lattice-based compilers (Gentry et al. CRYPTO 2006) in all aspects, hence yielding the most efficient aPAKE compiler from lattice. In particular, when applying our compiler to the UC-secure PAKE schemes (Santos et al. EUROCRYPT 2023, Beguinet et al. ACNS 2023), we obtain the most efficient UC-secure aPAKE schemes from lattice.
- Moreover, the instantiation of our compiler from the tightly-secure matrix DDH (MDDH)-based KEM (Pan et al. CRYPTO 2023) can compile the tightly-secure PAKE scheme (Liu et al. PKC 2023) to a tightly-secure MDDH-based aPAKE, which serves as the first tightly UC-secure aPAKE scheme.

**Keywords:** Password authenticated key exchange; asymmetric password authenticated key exchange; lattice; post-quantum security

#### 1 Introduction

Password Authenticated Key Exchange (PAKE) facilitates a secure establishment of session keys between two parties, say a client and a server, over a public network using a low entropy password pw. These session keys can then be used to set up secure communication channels for the client and server. In contrast to Authenticated Key Exchange (AKE) protocols, PAKE operates with easily memorable passwords and eliminates the need for reliance on Public Key Infrastructure (PKI), hence offering a more convenient deployments of secure channels.

Note that the adversary can always implement online invocations of the PAKE protocol with guessing passwords. The low entropy of the passwords might make such online attacks succeed with non-negligible probability. So the security of PAKE requires these online attacks be the only efficient attacks.

For PAKE, a password must be shared between the client and server. Generally, the password is memorable so it is not necessary for the client to store it. However, the server has to store passwords for all the clients. If the server is compromised, the adversary can snatch the password pw from the server so as to impersonate the client. To address this vulnerability, asymmetric PAKE (aPAKE) [15] was proposed. With an aPAKE, the server only has to store a password file, which is a one-way function value H(pw) of the password pw. Now if the server is compromised, the adversary only obtains the password file instead of the plain password. Therefore, aPAKE is deemed preferable to PAKE in the client-server setting. In this paper, we focus on aPAKE.

For aPAKE, if the adversary obtains H(pw), it is possible for him/her to implement a so-called offline attack: compute or pre-compute (pw', H(pw'))pairs to check the correctness of guessing password pw' by testing whether H(pw') = H(pw). Clearly, offline attack is inevitable after H(pw) is obtained by the adversary. As such, the security of aPAKE requires these offline attacks on H(pw) be the only efficient attacks that may work (beyond the online attacks).

Security Models for aPAKE. There are two types of security notions for aPAKE, the game-based security in the Indistinguishability model (IND security) [3,4] and the simulation-based security under the Universally Composable framework (UC security) [15]. The UC framework is preferable to the IND model in the following important aspects.

- The UC framework permits arbitrary correlations and distributions for passwords, while the IND model typically assumes passwords uniformly distributed over a dictionary for the sake of security proofs.
- Protocols that are proven secure in the UC framework enable a smooth and secure composition with other UC-secure protocols, thanks to the universal composition theorem [8].

Therefore, UC framework offers a more robust security guarantee and facilitates modular design of complex protocols, making it a better security model than the IND model.

**aPAKE from Post-Quantum Assumptions.** Now there is a trend to migrate cryptographic algorithms to post-quantum ones. In fact, NIST has already determined Kyber [7] as the Post-Quantum Cryptography (PQC) winner for Key Encapsulation Mechanism (KEM), and Dilithium [11], Falcon [14], Sphincs<sup>+</sup>[5] for digital signature schemes. Recently, the Crypto Forum Research Group (CFRG)

in IETF [31] initiated a selection process for both PAKE and aPAKE protocols. As far as we know, none of existing candidates are based on post-quantum assumptions.

There do exist a few aPAKE compilers instantiable from post-quantum assumptions. One compiler is the  $\Omega$ -method proposed by Gentry et al. [15], which can compile any UC-secure PAKE protocol into a UC-secure aPAKE protocol with the help of a signature scheme. Accordingly, the existing UC-secure PAKE protocol from lattices [29,2] and post-quantum secure signature schemes (like Dilithium [11], Falcon [14], Sphincs<sup>+</sup> [5]) admit UC-secure aPAKE protocols. Another compiler is due to McQuoid and Xu [24], which can compile any UCsecure PAKE protocol into a strong aPAKE protocol. This strong aPAKE is secure against pre-computation attacks (in idealized generic group action model [12]), but their compiler can only be instantiable from group actions (e.g. isogenybased CSIDH) rather than lattices. Note that there also exists an aPAKE compiler from UC-secure Key-Hiding AKE protocols [17,30,29]. However, no such key-hiding AKE protocols is instantiable from post-quantum assumptions. So up to now this compiler does not lead to post-quantum secure aPAKE yet.

In summary, the two UC-secure aPAKE compilers in [15,24] seem to be the only available approaches to aPAKE achieving post-quantum security. However, either compiler has its own limitations.

- The compiler in [24] can only be instantiated from isogeny-based assumptions, rather than the mainstream lattice-based assumptions. Besides, the isogeny-based group action does not offer good computational efficiency under the current parameter configuration.
- The compiler in [15] can be instantiated from lattice-based assumptions with the help of lattice-based signature schemes. However, it is not very efficient since current lattice-based signature schemes (like Dilithium [11] in the NIST PQC winner) will lead to much higher computational overhead compared to their KEM counterparts (like Kyber [7] in the NIST PQC winner) under the same security level. Technically speaking, this might be mainly due to the time-consuming process of trapdoor sampling or rejection sampling involved in most lattice-based signature schemes, dating back to the seminal works of [16,23].

This motivates us to seek a new aPAKE compiler instantiable from lattice to answer the following question:

> How to construct an efficient UC-secure aPAKE protocol from lattices, without using signatures?

**Our Contribution.** In this paper, we address the aforementioned question through the following contributions.

• UC-secure aPAKE compiler without using signatures. We propose a novel generic compiler that can compile any UC-secure PAKE protocol to a UC-secure aPAKE protocol, with the help of weak primitives of KEM and Authenticated Encryption (AE). KEM is only required to have One-Wayness under Plaintext-Checkable Attacks (OW-PCA)[25], weaker than the standard Indistinguishability under Chosen-Ciphertext Attacks (IND-CCA). AE is only required to have one-time CCA security and one-time authenticity, which has efficient information-theoretical instantiations. In particular, our compiler does not rely on signature schemes.

• Mutual explicit authentication & good round efficiency. In addition to its excellent efficiency, our compiler enjoys other desirable features. By using our compiler, the resulting aPAKE enjoys mutual explicit authentication even if the underlying PAKE does not. This is similar to the compiler in [15] but in sharp contrast to [24], which completely relies on the underlying PAKE to achieve mutual explicit authentication.

Moreover, our compiler only augments two additional rounds to the underlying PAKE. If the last round message of PAKE is sent from the server, then the first additional round of our compiler can be merged to the last round of PAKE, and hence only one additional round is needed for aPAKE. This is also similar to the compiler in [15] and comparable to [24].<sup>4</sup>

- The most efficient UC-secure aPAKE from lattice. By instantiating the KEM in our compiler with Kyber, the NIST PQC KEM winner, we obtain a lattice-based compiler. The performance evaluations show that our Kyber-based compiler outperforms the signature-based compiler in [15] from lattice in all aspects: ours save at least 61.1%-63.8% computing time and 41.5%-84.3% communication cost. Our Kyber-based compiler turns out to be the most efficient aPAKE compiler from lattice, and also results in *the most efficient UC-secure aPAKE schemes from lattice* when applying to the UC-secure PAKE schemes in [29,2].
- The first tightly UC-secure aPAKE. By instantiating the KEM in our compiler with the tightly-secure matrix DDH (MDDH)-based KEM scheme proposed in [26], we obtain a tightness-preserving compiler, which yields *the first tightly UC-secure aPAKE scheme* when applying the compiler to the tightly-secure PAKE scheme in [22].

**Technique Overview.** Our aPAKE compiler mainly relies on a KEM with OW-PCA security to compile a PAKE to an aPAKE protocol. Here OW-PCA [25] is weaker than IND-CCA security and asks one-wayness of ciphertext even if the adversary has access to a "plaintext-checking" oracle which on input a ciphertext-key pair (c, K) determines whether c is an encapsulation of K.

Our compiler also requires a one-time secure Authenticated Encryption (AE) and five hash function  $H_0, \dots, H_4$ . Here one-time security of AE includes one-time authenticity and one-time CCA security. We note that one-time secure AE has very efficient information-theoretical instantiations, e.g., from one-time pad and one-time secure message authentication code (MAC). On the other hand,

<sup>&</sup>lt;sup>4</sup> More precisely, the compiler in [24] incurs an additional round from server to client before PAKE. Since it is usually the client who starts the protocol, actually two additional rounds are needed before PAKE in [24].

the hash functions will be modelled as Random Oracles (RO) during the security proof.

We refer to Fig. 1 for a high-level description of our compiler. More precisely, our compiler works as follows.

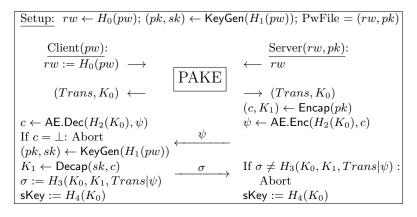


Fig. 1: High level description of our aPAKE compiler from KEM and AE.

The server's password file contains a hash value  $H_0(pw)$  of the password pwand a KEM public key pk, which is derived from the password pw by using  $H_1(pw)$  as the randomness of key generation, i.e.,  $(pk, sk) \leftarrow \mathsf{KeyGen}(H_1(pw))$ .

To establish a session key sKey, the client and server equip the underlying PAKE with password  $rw = H_0(pw)$ , and run the PAKE protocol to derive a PAKE session key  $K_0$ .

Next, the server will use KEM to distribute a key  $K_1$  to the client with the help of pk (retrieved from its password file): it first invokes  $(c, K_1) \leftarrow \mathsf{Encap}(pk)$ but it does not send c directly to the client. Instead, the server will use the PAKE session key  $K_0$  to derive a key  $H_2(K_0)$  for AE. Then with the help of AE, the server further encrypts the encapsulation c to obtain an AE ciphertext  $\psi$  via  $\psi \leftarrow \mathsf{AE}.\mathsf{Enc}(H_2(K_0), c)$ , and sends  $\psi$  to the client. In this way, the (one-time) authenticity of AE helps the server authenticate itself to the client since only the server and client can compute  $K_0$  via PAKE and generate valid ciphertext  $\psi$ (i.e., the decryption of which does not lead to rejection) under AE key  $H_2(K_0)$ .

After receiving  $\psi$ , the client checks the validity of  $\psi$  with the AE key  $H_2(K_0)$ . If  $\psi$  is valid, i.e., AE.Dec $(H_2(K_0), \psi) \neq \bot$ , the client will set the session key  $\mathsf{sKey} := H_4(K_0)$ . It also recovers the KEM secret key sk from pw via  $(pk, sk) \leftarrow$  KeyGen $(H_1(pw))$ , and then double decrypts  $\psi$  with AE key  $H_2(K_0)$  and KEM secret key sk to obtain  $K_1$ . Finally, the client computes an authenticator  $\sigma :=$   $H_3(K_0, K_1, Trans | \psi)$  where Trans is the transcription of PAKE, and sends  $\sigma$  to the server. Note that only the server and client can compute  $K_0$  and  $K_1$ . In this way, the confidentiality of KEM and AE (i.e., OW-PCA of KEM and one-time CCA of AE) help the client authenticate itself to the server. Finally, the server checks the validity of  $\sigma$  with  $(K_0, K_1)$  by testing whether  $\sigma = H_3(K_0, K_1, Trans|\psi)$ , where  $Trans, \psi, \sigma$  constitute the transcription seen by the server. If  $\sigma$  is valid, the server's session key is set to  $\mathsf{sKey} := H_4(K_0)$ .

Roughly speaking, our aPAKE compiler is designed in a "PAKE plus passwordbased mutual authentication" manner. PAKE helps the client and server share an AE key  $H_2(K_0)$  and then AE helps the authentication of the server. Meanwhile, the server's message  $\psi$  can be viewed as a "challenge" to the client. Only the client knowing the correct password pw is able to derive the KEM secret key sk to recover  $K_1$  and generate the correct "response"  $\sigma$  with  $(K_0, K_1)$ . Putting differently,  $\sigma$  can be viewed as a proof of knowledge of pw for the client. As long as adversary  $\mathcal{A}$  does not obtain pw through offline or online attacks,  $\mathcal{A}$  cannot impersonate the client even if  $\mathcal{A}$  compromises the server and obtains (rw, pk).

**UC security in RO model.** To prove the UC security for our aPAKE compiler in the random oracle (RO) model, we have to construct a simulator Sim to simulate all the interaction transcripts and session keys for both passive and active attacks implemented by  $\mathcal{A}$ , without the knowledge of password pw but accessing to the ideal functionality  $\mathcal{F}_{apake}$  for aPAKE (see Fig. 4 in Sect. 2.3).

The aPAKE protocol has two parts: the PAKE part in which  $rw = H_0(pw)$ is used to generate PAKE key  $K_0$ , and the last two rounds in which  $K_0$  and (pk, sk, rw) are used to generate  $\psi$ ,  $\sigma$  and the session keys sKey. Recall that PAKE has UC security, so the PAKE part can emulate the ideal functionality  $\mathcal{F}_{pake}$  (see Fig. 3 in Sect. 2.3 for the description of  $\mathcal{F}_{pake}$ ).

Firstly, let us consider  $\mathcal{A}$ 's attacks on the PAKE part. The task of Sim is to simulate the correctly distributed PAKE key  $K_0$  without password pw. Note that if  $\mathcal{A}$  did not use the correct PAKE password  $rw := H_0(pw)$  in the PAKE part,  $\mathcal{A}$ 's active attack on the PAKE part hardly succeeds, due to the ideal functionality  $\mathcal{F}_{pake}$  of PAKE. We consider the following three cases.

- Case I:  $\mathcal{A}$ 's successful active attacks on the PAKE part with the correct password pw. In this case,  $\mathcal{A}$  successful implements either an online attack or an offline attack, in both of which  $\mathcal{A}$  must have queried  $H_0(pw)$  to obtain rw. For  $\mathcal{A}$ 's such an attack with rw, Sim can search the hash list to find pw' such that  $rw = H_0(pw')$ , and then justify the correctness of pw' with the help of Testpw interface of  $\mathcal{F}_{apake}$ . In this way, Sim is able to extract the correct password pw from  $\mathcal{A}$ 's successful active attacks. Then with pw, it can simulate the PAKE part to generate PAKE key  $K_0$  for  $\mathcal{A}$ .
- Case II:  $\mathcal{A}$ 's successful active attacks on the PAKE part with the stolen PAKE password rw. In this case,  $\mathcal{A}$  must have stolen the password file (rw, pk) and can use rw to impersonate client or server in the PAKE part of the aPAKE protocol. Sim can simulate the generation of password file for  $\mathcal{A}$  with random elements. More precisely, Sim picks rw and rrandomly, sets  $H_0(?) := rw$  and  $H_1(?) := r$  respectively with pw = ? undetermined, and generates  $(pk, sk) \leftarrow \text{KeyGen}(r)$ . If later  $\mathcal{A}$  attacks with correct pw, Sim can extract it (see Case I) and then re-program the hash function with  $H_0(pw) := rw$  and  $H_1(pw) := r$ . With the knowledge of rw,

it can simulate  $\mathcal{F}_{pake}$  to generate PAKE key  $K_0$  for  $\mathcal{A}$ . We stress that Sim generates (pk, sk, rw) without pw in this case.

- Case III: the other cases. If neither Case I nor Case II happens, then either  $\mathcal{A}$ 's active attack fails or  $\mathcal{A}$  implements a passive attack.
  - **Case III.1: Failed active attack on the PAKE part.** In this case, either the PAKE part outputs  $\perp$  to abort the protocol (PAKE with explicit authentication), or the PAKE part outputs different PAKE session keys  $K_0$  and  $K'_0$  for Client and Server respectively (PAKE with implicit authentication), where  $K_0$  and  $K'_0$  must be uniform to  $\mathcal{A}$  according to the UC security of PAKE.
  - Case III.2: Passive attack on the PAKE part. In this case, the PAKE part generates the shared PAKE session key  $K_0$  for Client and Server. According to the UC security,  $K_0$  must be uniform to  $\mathcal{A}$ .
  - In this case, Sim can simulate  $K_0$  (also  $K'_0$ ) with a randomly chosen one.

Next, let us consider  $\mathcal{A}$ 's attacks on the last two rounds of the aPAKE protocol. We follow the above three cases.

- **Case I happened.** In this case, Sim has extracted the correct password pw and also knows PAKE key  $K_0$ . With the knowledge of pw and  $K_0$ , Sim can give a perfect simulation for  $\mathcal{A}$ 's active attacks (here passive attack is impossible due to the previous active attack on the PAKE part) with round message  $\psi'$  or  $\sigma'$ . Note that Sim can use the correct pw to invoke  $\mathcal{F}_{apake}$  to assign the session key sKey determined by  $\mathcal{A}$  to both client and server.
- **Case II happened.** In this case, Sim has the knowledge of (pk, sk, rw) itself (generated without pw) and the PAKE key  $K_0$ . also uniformly distributed.
  - For  $\mathcal{A}$ 's active attack with  $\psi'$ , Sim can determine the validity of  $\psi'$  with  $K_0$ . It rejects  $\psi'$  and aborts the protocol for invalid  $\psi'$ , and for valid  $\psi'$  it invokes  $\mathcal{F}_{apake}$  to assign the session key sKey determined by  $\mathcal{A}$  to both client and server (dealing with the case that  $\mathcal{A}$  stole the file (pk, rw) and successfully impersonated server to accomplish the aPAKE protocol).
  - For  $\mathcal{A}$ 's active attack with  $\sigma'$ , Sim can determine the validity of  $\sigma'$  with  $K_0$  and  $K_1$ . If  $\sigma'$  is valid and  $\mathcal{A}$  has obtained the correct password pw via an offline attack, it invokes  $\mathcal{F}_{apake}$  to assign the session key sKey determined by  $\mathcal{A}$  to both client and server. If  $\sigma'$  is invalid, it rejects  $\sigma'$  and aborts the protocol. Define Bad as the event that  $\sigma'$  is valid but  $\mathcal{A}$  did not obtain pw from offline attack. If Bad happens, it rejects  $\sigma'$  as well. However in the real experiment, in case of Bad,  $\sigma'$  should be accepted. This imperfect simulation does not annoy us since Bad can hardly happen, which is guaranteed by the OW-PCA security of KEM. The reason is as follows. Without pw,  $\mathcal{A}$  cannot derive sk, then  $\mathcal{A}$  cannot obtain  $K_1$  due to the OW-PCA security, hence  $H_3(K_0, K_1, Trans | \psi)$  is uniform to  $\mathcal{A}$  and  $\sigma' = H_3(K_0, K_1, Trans | \psi)$  hardly holds.
- **Case III happened.** In this case, Sim has the knowledge of  $K_0$  which is uniformly distributed in  $\mathcal{A}$ 's view. Then to  $\mathcal{A}$ , the hash values of  $H_2(K_0)$ ,  $H_3(K_0, K_1, Trans|\psi)$ ,  $H_4(K_0)$  are also uniformly distributed.

- For  $\mathcal{A}$ 's passive attacks on server or client, Sim can simulate  $\psi$  with  $\psi \leftarrow \mathsf{AE}.\mathsf{Enc}(H_2(K_0), \text{dummy message})$  and simulate  $\sigma$  with a uniform string, and invoke  $\mathcal{F}_{apake}$  to generate random session key sKey for server or client. Given uniform AE key  $H_2(K_0)$ , AE encryption of a dummy message is indistinguishable from AE encryption of the real message c, due to the one-time CCA security of AE. Meanwhile random oracles guarantee the uniformity of  $\sigma := H_3(K_0, K_1, Trans | \psi)$  and sKey :=  $H_4(K_0)$ . Moreover, Sim invokes  $\mathcal{F}_{apake}$  to generate a uniform session key sKey for both client and server. Therefore, Sim's simulation is perfect for these passive attacks.
- For  $\mathcal{A}$ 's active attacks on client with  $\psi'$ , Sim directly rejects and aborts the protocol. Without the knowledge of AE key  $H_2(K_0)$ ,  $\mathcal{A}$ 's forgery of  $\psi'$ will result in AE.Dec $(H_2(K_0), \psi') = \bot$ , due to the one-time authenticity of AE. So Sim's simulation of dealing with  $\psi'$  is perfect (except with negligible probability).
- For  $\mathcal{A}$ 's active attacks on client with  $\sigma'$ , Sim directly rejects and aborts the protocol. Without the knowledge of KEM's secret key sk,  $K_0$ ,  $\mathcal{A}$ 's forgery of  $\sigma'$  can hardly collide with the valid  $\sigma := H_3(K_0, K_1, Trans|\psi)$ , due to uniformity of the RO outputs. So Sim's simulation of dealing with  $\psi'$  is perfect (except with negligible probability).

**Comparison.** In Table 1, we instantiate our aPAKE compiler with the NIST PQC KEM winner algorithm Kyber, and compare it with the signature-based compiler [15], which is the only known aPAKE compiler instantiable from lattices prior to our work. The performance results in Table 1 is obtained by running experiments on Intel(R) Core(TM) i7-1068NG7 CPU @ 2.30GHz with 4 cores under macOS 13.3.1. When the compiler [15] is instantiated with the NIST PQC lattice-based signature scheme Dilithium or Falcon, our compiler significantly outperforms theirs in all aspects including registration time, computing time, server storage size, and communication cost. This suggests that our compiler is the most efficient aPAKE compiler from lattices. As far as we know, there is no UC-secure aPAKE scheme constructed directly from lattices, and the only approach to UC-secure aPAKE from lattices is via compiling a PAKE scheme to an aPAKE. Therefore, the good efficiency of our compiler suggests that applying our compiler to the available UC-secure PAKE schemes from lattices will yield the most efficient UC-secure aPAKE schemes from lattices.

We also compare our compiler with known aPAKE compilers [15,24] instantiated from other post-quantum assumptions (see Table 3 in Appendix D). The comparison shows that our compiler overwhelms these compilers in terms of registration time and computing time, and has comparable server storage and communication cost.

In Table 2, we also compare the resulting MDDH-based aPAKE scheme (from our MDDH-based compiler) with other aPAKE schemes in terms of tight UC security. The tight security of aPAKE in [22,30,32,19,24] is eliminated by the impossibility result in [22], which essentially said that tightly UC-security is impossible to achieve if the secret derived from password by client is uniquely Table 1: Efficiency comparison of our Kyber-based compiler with the other aPAKE compilers [15] from lattices, where Kyber is in its version of NIST security level 3. For computing and communication cost, we use the mode of "Client + Server = Total" to reflect the seperation of client/server computation/communication. The aPAKE compiler in [15] has two lattice-based instantiations, one is instantiated with Dilithium in its version of NIST security level 3, and the other is instantiated with Falcon in its version of NIST security level 1 (due to its lack of level 3).

aPAKE Compiler	Registration Time (ms)	* 0	Server Storage (KB)	Communication Cost (KB)	Assumption Type
[15] (Dilithium)	0.096	0.245 + 0.126 = 0.371	5.875	3.215 + 3.938 = 7.153	Lattice-based
[15] (Falcon)	7.003	0.271 + 0.074 = 0.345	2.189	0.642 + 1.282 = 1.924	Lattice-based
Ours (Kyber)	0.017	0.051 + 0.083 = 0.134	1.188	0.031 + 1.094 = 1.125	Lattice-based

Table 2: Comparison of our MDDH-based aPAKE scheme with other UC-secure aPAKE scheme in terms of tight UC security, where our aPAKE scheme is resulted from compiling the PAKE protocol [22] with our MDDH-based compiler. "?" denotes its tight UC security is unknown.

aPAKE scheme	Our MDDH-based aPAKE	[22]	[30]	[32]	[19]	[24]	[15]	[17]
Tight UC Security?	$\checkmark$	×	×	×	×	×	?	?

determined by the password file and moreover the relation between the secret and file can be efficiently determined. In contrast to their schemes, the client secret (rw, sk) in our MDDH-based aPAKE evades the impossibility result since the key generation of MDDH-based KEM makes sure that multiple sk correspond to one pk and hence to one password file. On the other hand, the aPAKE schemes [15,17] in Table 2 are obtained by compiling PAKE + signature in [15] and AKE + ideal cipher in [17] respectively, but the security reduction is not tight, so it is unknown whether tight UC security can be achieved.

The Necessity of AE in Our Compiler. Note that AE plays an important role in our compiler for aPAKE to achieve explicit authentication. Moreover, AE is especially necessary in our compiler when the underlying KEM has no anonymity under secret key leakage. No anonymity under secret key leakage means that given sk, one can efficiently decide whether a KEM ciphertext c is generated under pk. If we take off AE from the round messge  $\psi$ , the server will send the KEM ciphertext c directly, and then the resulting aPAKE will suffer from an offline attack: the adversary sees the encapsulation c, tries different password pw, generates  $(pk, sk) \leftarrow \text{KeyGen}(H_1(pw))$ , and tests whether c is the KEM ciphertext generated under key pair (pk, sk).

As far as we know, many lattice-based KEMs have no anonymity under secret key leakage. Let us take Regev's encryption scheme [28] as an example. For a ciphertext c generated under pk, the decryption of c using sk will result in a value which is either very close to 0 or close to q/2 with q the modulus. However, for c generated under another public key pk', the decryption of c using sk may result in a value far from both 0 and q/2. In this way, one can in fact efficiently tell whether c is generated under pk (at least with noticeable probability). Consequently, AE is necessary for our lattice-based compiler.

On the other hand, if the underlying KEM does have anonymity under secret key, which means the adversary cannot distinguish a given ciphertext c is generated under  $(pk_1, sk_1)$  or  $(pk_2, sk_2)$ , the above offline attack fails. However, the price of getting rid of AE from our compiler is that we lose the explicit authentication of server-side. Actually, the CDH-based aPAKE compiler [19] can be seen as an instantiation of our compiler from ElGamal KEM without AE, and of course the CDH-based aPAKE does not achieve explicit mutual authentication.

Hardness on Achieving UC-Secure aPAKE in QROM. Note that our aPAKE compiler is proved under ROM instead of Quantum Random Oracle Model (QROM) [6]. QROM allows adversary  $\mathcal{A}$  to perform superposition queries to random oracles, making it hard for simulator to extract preimages or reprogram random oracles. It is especially hard to give UC-secure aPAKE protocols in QROM since reprogrammable random oracles are unavoidable for the construction of UC-secure aPAKE protocols, as demonstrated in [18]. Therefore, it is a big challenge to construct UC-secure aPAKE in QROM, and we leave it as an interesting open problem.

#### 2 Preliminary

Let  $\lambda \in \mathbb{N}$  denote the security parameter throughout the paper. If x is defined by y or the value of y is assigned to x, we write x := y. For  $\mu \in \mathbb{N}$ , define  $[\mu] := \{1, 2, \ldots, \mu\}$ . Denote by  $x \leftarrow_{\mathbb{S}} \mathcal{X}$  the procedure of sampling x from set  $\mathcal{X}$  uniformly at random. Let  $|\mathcal{X}|$  denote the number of elements in  $\mathcal{X}$ . All our algorithms are probabilistic unless stated otherwise. We use  $y \leftarrow \mathcal{A}(x)$  to define the random variable y obtained by executing algorithm  $\mathcal{A}$  on input x. We also use  $y \leftarrow \mathcal{A}(x; r)$  to make explicit the random coins r used in the probabilistic computation. The notation " $\approx_s$ " represents statistical indistinguishability, while " $\approx_c$ " denotes computational indistinguishability. "PPT" abbreviates probabilistic polynomial-time. Denote by negl some negligible function.

In Subsect. 2.1, we recall the definitions of Key Encapsulation Mechanism (KEM), Authentication Encryption (AE) and their security notions. In Subsect. 2.2 and Subsect. 2.3, we present the ideal functionalities of random oracle and (a)PAKE, respectively.

#### 2.1 KEM and AE

**Definition 1 (KEM).** A key encapsulation mechanism (KEM) scheme KEM = (KeyGen, Encap, Decap) consists of three algorithms:

- KeyGen(r): Taking as input a randomness  $r \in \mathcal{R}$ , the key generation algorithm outputs a pair of public key and secret key (pk, sk).

- $\mathsf{Encap}(pk)$  : Taking as input a public key pk, the encapsulation algorithm outputs a pair of ciphertext  $c \in CT$  and encapsulated key  $K \in K$ .
- Decap(sk, c): Taking as input a secret key sk and a ciphertext c, the decapsulation algorithm outputs  $K \in \mathcal{K}$ .

The correctness of KEM requires that

$$\Pr \begin{bmatrix} r \leftarrow_{\mathrm{s}} \mathcal{R}, (pk, sk) \leftarrow \mathsf{KeyGen}(r) \\ (c, K) \leftarrow \mathsf{Encap}(pk) \end{bmatrix} : \mathsf{Decap}(sk, c) = K \end{bmatrix} = 1 - \mathsf{negl}(\lambda).$$

**Definition 2 (OW-PCA security for KEM).** For a KEM scheme KEM = (KeyGen, Encap, Decap), the advantage function of an adversary A is defined by

where the oracle CHECK takes as input a ciphertext-key pair (c, K) and returns whether  $\mathsf{Decap}(sk, c) = K$  or not. The OW-PCA security for KEM requires  $\mathsf{Adv}_{\mathsf{KEM}}^{\mathsf{ow-pca}}(\mathcal{A}) = \mathsf{negl}(\lambda)$  for all PPT  $\mathcal{A}$ .

**Definition 3 (AE).** An authenticated encryption (AE) scheme AE = (Enc, Dec) consists of two algorithms:

- Enc(k, m): Taking as input a key  $k \in \mathcal{K}$  and a message  $m \in \mathcal{M}$ , the encryption algorithm outputs a ciphertext c.
- Dec(k, c): Taking as input a key  $k \in \mathcal{K}$  and a ciphertext c, the decryption algorithm outputs a message  $m \in \mathcal{M}$  or a symbol  $\perp$ .

The correctness of AE requires that Dec(k, Enc(k, m)) = m holds for all  $k \in \mathcal{K}$ and all  $m \in \mathcal{M}$ .

**Definition 4 (One-time authenticity for AE).** For an AE scheme AE = (Enc, Dec), the advantage function of an adversary  $\mathcal{A}$  for one-time authenticity is defined by  $Adv_{AE}^{ot-auth}(\mathcal{A}) := \Pr \left[ k \leftarrow \mathcal{K}, c \leftarrow \mathcal{A}^{ENC(k,\cdot)} : Dec(k,c) \neq \bot \land c \text{ is not the output of oracle <math>Enc(k,\cdot) \right]$ . The one-time authenticity for AE requires  $Adv_{AE}^{ot-auth}(\mathcal{A}) = negl(\lambda)$  for all PPT  $\mathcal{A}$  that query the oracle  $ENC(k,\cdot)$  at most once.

**Definition 5 (One-time IND-CCA security for AE).** For an AE scheme AE = (Enc, Dec), the advantage function of an adversary  $\mathcal{A}$  for one-time CCA security is defined by  $Adv_{AE}^{ot-cca}(\mathcal{A}) := |\Pr[k \leftarrow s \mathcal{K}, b \leftarrow s \{0,1\}, (m_0, m_1) \leftarrow \mathcal{A}^{Dec(k,\cdot)}, c_b \leftarrow Enc(k, m_b), b' \leftarrow \mathcal{A}^{Dec(k,\cdot)}(c_b) : b = b'] - 1/2|$ . The one-time IND-CCA security requires  $Adv_{AE}^{ot-cca}(\mathcal{A}) = negl(\lambda)$  for all PPT  $\mathcal{A}$  that query the oracle  $Dec(k, \cdot)$  at most once for a ciphertext different from  $c_b$ .

Such an AE can be easily constructed from one-time pad and one-time secure Message Authentication Code (MAC), and hence it has a very efficient information-theoretical instantiation. See Sect. 4 for the detailed construction.

#### 2.2 Idealized Random Oracle Model

The idealized functionality of random oracle is shown in Fig. 2. The idealized functionality of random oracle can be perfectly simulated by a PPT simulator Sim: Sim maintains a list  $\mathcal{L}$  (initialized to be empty) to store the records. Upon receiving a query (Eval, x) from P, Sim checks whether there exists  $(x, y) \in \mathcal{L}$ . If yes, Sim returns y. Otherwise, Sim randomly samples  $y \leftarrow_{s} \mathcal{Y}$ , records (x, y) in the list  $\mathcal{L}$ , and returns y.

Ideal Functionality $\mathcal{F}_{RO}$
The ideal functionality $\mathcal{F}_{RO}$ is parameterized by a random map $H: \{0,1\}^* \to \mathcal{Y}$ .
Upon receiving a query $(Eval, x)$ from P:
If $H(x)$ is defined: return $H(x)$ .
Else: $y \leftarrow \mathcal{Y}, H(x) := y$ , return $H(x)$ .

Fig. 2: The ideal functionality  $\mathcal{F}_{RO}$  for random oracle H.

#### 2.3 (Asymmetric) PAKE under UC Framework

In Fig. 3 and Fig. 4, we show the ideal functionalities of PAKE and aPAKE respectively. Here the functionalities mainly follows from [15] along with some modifications as did in [32]. The ideal functionality of aPAKE is extended from that of PAKE, so we only explain aPAKE below.

Functionality  $\mathcal{F}_{pake}$ The functionality  $\mathcal{F}_{pake}$  is parameterized by a security parameter  $\lambda$ . It interacts with an adversary  $\mathcal{A}$ and a set of parties via the following queries: Upon receiving a query (NewClient,  $C^{(i)}$ , *iid*,  $S^{(j)}$ , *pw*) from  $C^{(i)}$ : Send (NewClient,  $C^{(i)}$ , *iid*,  $S^{(j)}$ ) to A. Record ( $C^{(i)}$ , *iid*,  $S^{(j)}$ , *pw*) and mark it as fresh. Upon receiving a query (NewServer,  $S^{(j)}$ , iid',  $C^{(i)}$ , pw) from  $S^{(j)}$ : Send (NewServer,  $S^{(j)}$ , iid',  $C^{(i)}$ ) to  $\mathcal{A}$ . Record  $(S^{(j)}, iid', C^{(i)}, pw)$  and mark it as fresh. Upon receiving a query (Testpw, P, iid, pw') from A: If there is a **fresh** record  $(P, iid, \cdot, pw)$ : If pw' = pw, mark the record **compromised** and reply to  $\mathcal{A}$  with "correct guess". If  $pw' \neq pw$ , mark the record **interrupted** and reply  $\mathcal{A}$  with "wrong guess". Upon receiving a query (NewKey, P, *iid*, *sid*, Key<sup>\*</sup>) from A: If there is a **compromised** record (P, iid, Q, pw), send  $(sid, Key^*)$  to P. If there is a **fresh** record (P, iid, Q, pw), there is a **completed** record (Q, iid', P, pw') with pw = pw' $\mathcal{F}_{pake}$  has sent  $(sid, \mathsf{Key'})$  to Q, and (Q, iid', P, pw') was **fresh** when  $(sid, \mathsf{Key'})$  was sent, then output (sid, Key') to P. In any other case, pick a new random key Key  $\leftarrow$  s  $\{0,1\}^{\lambda}$  and send (sid, Key) to P. In all cases, mark the record (P, iid, Q, pw) as **completed**.

Fig. 3: The ideal functionality  $\mathcal{F}_{pake}$  for PAKE.

Security guarantees in the ideal world.  $\mathcal{F}_{apake}$  in Fig. 4 formalizes the ideal functionality of asymmetric PAKE with mutual explicit authentication.

#### Functionality $\mathcal{F}_{apake}$

٦

Functionality $\mathcal{F}_{apake}$
The functionality $\mathcal{F}_{apake}$ is parameterized by a security parameter $\lambda$ . It interacts with an adversary $\mathcal{A}$
and a set of parties via the following queries:
Password Storage
Upon receiving a query (StorePWFile, $C^{(i)}, S^{(j)}, pw$ ) from $S^{(j)}$ :
Record (file, $C^{(i)}, S^{(j)}, pw$ ), mark it as <b>fresh</b> , and send (StorePWFile, $C^{(i)}, S^{(j)}$ ) to $A$ .
Stealing Password File
Upon receiving a query (StealPWFile, $C^{(i)}, S^{(j)}$ ) from $\mathcal{A}$ :
Mark record (file, $C^{(i)}, S^{(j)}, pw$ ) as compromised, and send (StealPWFile, $C^{(i)}, S^{(j)}$ ) to $A$ .
If there is a record (offline, $C^{(i)}, S^{(j)}, pw'$ ) with $pw' = pw$ : send $pw$ and "correct guess" to $A$ .
Upon receiving a query (OfflineTestPW, $C^{(i)}, S^{(j)}, pw'$ ) from $\mathcal{A}$ :
If there exists a record (file, $C^{(i)}, S^{(j)}, pw$ ) marked <b>compromised</b> :
If $pw' = pw$ , return "correct guess", else return "wrong guess".
Else: Store (offline, $C^{(i)}, S^{(j)}, pw'$ ).
Sessions
Upon receiving a query (NewClient, $C^{(i)}$ , <i>iid</i> , $S^{(j)}$ ) from $C^{(i)}$ :
Retrieve the record (file, $C^{(i)}$ , $S^{(j)}$ , $pw$ ).
Send (NewClient, $C^{(i)}$ , $iid$ , $S^{(j)}$ ) to $\mathcal{A}$ . Record ( $C^{(i)}$ , $iid$ , $S^{(j)}$ , $pw$ ) and mark it as <b>fresh</b> .
Upon receiving a query (NewServer, $S^{(j)}$ , $iid'$ , $C^{(i)}$ ) from $S^{(j)}$ :
Retrieve the record (file, $C^{(i)}, S^{(j)}, pw$ ). Send (NewServer, $S^{(j)}, iid', C^{(i)}$ ) to $\mathcal{A}$ .
Record $(S^{(j)}, iid, C^{(i)}, pw)$ and mark it as <b>fresh</b> .
Active Session Attacks
Upon receiving a query (Testpw, $P, iid, pw'$ ) from $\mathcal{A}$ :
If there is a <b>fresh</b> record $(P, iid, \cdot, pw)$ :
If $pw' = pw$ , mark the record <b>compromised</b> and reply to $\mathcal{A}$ with "correct guess".
If $pw' \neq pw$ , mark the record <b>interrupted</b> and reply to $\mathcal{A}$ with "wrong guess".
Upon receiving a query (Impersonate, $C^{(i)}$ , <i>iid</i> ) from $\mathcal{A}$ :
If there exists a record (file, $C^{(i)}, S^{(j)}, pw$ ) marked <b>compromised</b> and a record ( $C^{(i)}, iid, S^{(j)}, pw$ )
marked <b>fresh</b> :
mark the record $(C^{(i)}, iid, S^{(j)}, pw)$ compromised and return "correct guess" to $\mathcal{A}$ .
Otherwise, mark the record $(C^{(i)}, iid, S^{(j)}, pw)$ interrupted and return "wrong guess" to $A$ .
Key Generation
Upon receiving a query (FreshKey, $P$ , $iid$ , $sid$ ) from $A$ :
If there is a <b>fresh</b> record $(P, iid, Q, pw)$ and sid has never been assigned to P's any other instance: Bids $f(w) \in \{0, 1\}$ and $f(Q, pw)$ and $f(Q, pw)$ as group let $d$ actume $(wid, f(w))$ to $P$ and
Pick sKey $\leftarrow$ s $\{0, 1\}^{\lambda}$ , mark the record $(P, iid, Q, pw)$ as <b>completed</b> , return $(sid, sKey)$ to P, and record $(P, Q, sid, sKey)$ .
Upon receiving a query (CopyKey, $P$ , $iid$ , $sid$ ) from $A$ :
If there is a <b>fresh</b> record $(P, iid, Q, pw)$ , a <b>completed</b> record $(Q, iid', P, pw)$ and <i>sid</i> has never
been assigned to $P$ 's any other instance:
If there exists record $(Q, P, sid, sKey)$ and the record $(Q, iid', P, pw)$ was <b>fresh</b> when Q receives
(sid, sKey): Mark the record $(P, iid, Q, pw)$ as <b>completed</b> , and return $(sid, sKey)$ to P.
Upon receiving a query (CorruptKey, <i>P</i> , <i>iid</i> , <i>sid</i> , <i>s</i> Key) from <i>A</i> :
If there is a <b>compromised</b> record $(P, iid, Q, pw)$ and sid has never been assigned to P's any other
instance: Mark the record $(P, iid, Q, pw)$ as <b>completed</b> , and return $(sid, sKey)$ to P.
Upon receiving a query (Abort, $P$ , <i>iid</i> ) from $A$ :
Mark the record $(P, iid, \cdot, pw)$ as <b>abort</b> , and return $(\bot, \bot)$ to P.

Fig. 4: The ideal functionality  $\mathcal{F}_{apake}$  for aPAKE.

Roughly speaking, the ideal functionally  $\mathcal{F}_{apake}$  in the UC model captures the following security guarantees in the ideal world.

- Passive attack and forward security. For a passive attacker  $\mathcal{A}$ , the session key is uniformly distributed (which is modeled by the FreshKey and CopyKey query), even if the adversary is given the password.
- Online guessing password attack. In this case, the adversary  $\mathcal{A}$  guesses a password pw' once for a session and tests whether his guess is correct, which is modeled by the Testpw query. This means that any active attack implemented by a real-world adversary  $\mathcal{A}$  to the protocol can be translated to a single Testpw query in the ideal world. If the password-guess is correct, then the adversary can control the session key at its will (which is modeled by the CorruptKey query). Otherwise, the attacked party can detect the active attack and reject this session directly (which modeled by the Abort query).
- Online impersonation attack on server after stealing the password file. In this case, the adversary  $\mathcal{A}$  has obtained the password file stored in the server. Without loss of generality, we write the password file as H(pw). With H(pw),  $\mathcal{A}$  can impersonate a server perfectly to communicate with a client, which is modeled by the Impersonate query. Besides online attack,  $\mathcal{A}$  can also implement offline attacks by choosing a password pw' and checking whether H(pw') = H(pw), which is modeled by the OfflineTestPW query. Moreover, before  $\mathcal{A}$  obtains the password file H(pw),  $\mathcal{A}$  can precompute a table of possible pairs (pw', H(pw')). When  $\mathcal{A}$  obtains the password file, he can search pw in the table quickly by comparing H(pw') = H(pw). This is also captured by the OfflineTestPW. Note that in this case,  $\mathcal{A}$  cannot impersonate a client unless  $\mathcal{A}$  makes a correct online password guess, or  $\mathcal{A}$  obtains the password via offline attacks, i.e.  $\mathcal{A}$  gets a pw' s.t. H(pw') = H(pw).

UC security for aPAKE. In the real world, the environment  $\mathcal{Z}$  has all passwords for all users, controls the adversary  $\mathcal{A}$ , and sees all the interactions over the channel and session keys derived from the protocol. In UC framework, we will construct a PPT simulator Sim which has access to the ideal functionality  $\mathcal{F}_{apake}$  and interacts with the environment  $\mathcal{Z}$ . If the view simulated by Sim for environment  $\mathcal{Z}$  is indistinguishable to  $\mathcal{Z}$ 's view in the real world, then UC security is achieved.

Difference between our  $\mathcal{F}_{pake}/\mathcal{F}_{apake}$  and the original  $\mathcal{F}_{pake}/\mathcal{F}_{apake}$ . The original ideal functionality  $\mathcal{F}_{pake}$  for PAKE was proposed in [9]. The ideal functionality  $\mathcal{F}_{apake}$  for aPAKE in [15] was built upon [9]. Shoup [32] improved and optimized both  $\mathcal{F}_{pake}$  and  $\mathcal{F}_{apake}$  in several ways.

- In the original ideal functionality  $\mathcal{F}_{pake}$  and  $\mathcal{F}_{apake}$ , each protocol instance must be identified by a globally unique session identifier and the PAKE participants can successfully establish a joint session key only if they use the same session identifier *sid*. The requirements on *sid* are problematic for an implementer, as pointed out by [1]. Shoup's modified  $\mathcal{F}_{pake}$  addresses this issue by replacing globally unique session identifiers with locally unique instance identifiers (iid), and session identifiers (sid) are seen as protocol outputs.

- The  $\mathcal{F}_{apake}$  in [15] is flawed, as pointed out by [18]. In fact, Shoup also pointed it out, and he fixed these flaws with a modified  $\mathcal{F}_{apake}$ .
- $\mathcal{F}_{apake}$  in [32] models the explicit authentication (via fresh-key, copy-key, corrupt-key and abort interfaces), while the formulation of explicit authentication in [15] is flawed, as pointed out by Remark 10 in [32].

In our paper, we adopt the optimized  $\mathcal{F}_{pake}$  and  $\mathcal{F}_{apake}$  provided in [32].

Remark 1. In this paper, we assume that each instance of a party (client or server) is initialized with the different instance ID *iid*. This is reasonable and also taken in [32] (see Sect. 4.3). Another notation is that for simplicity, our ideal functionality  $\mathcal{F}_{apake}$  does not model the case that client mistypes its password, but this can be easily taken into account with the same approach in [32] (See Remark 3 and Remark 4 in [32] for more details).

#### 3 Our aPAKE Compiler from KEM and AE

In this section, we propose an aPAKE compiler from KEM and AE, and show how to construct aPAKE from UC-secure PAKE with the help of our compiler in the UC framework. The detailed compiler (as well as the aPAKE construction) is shown in Fig. 5. Due to its UC security, PAKE can emulate its ideal functionality  $\mathcal{F}_{pake}$ , so we replace PAKE with  $\mathcal{F}_{pake}$  in the aPAKE construction.

Clearly, the resulting aPAKE scheme from our compiler is correct if the underlying PAKE, KEM and AE scheme are correct. If the underlying KEM has OW-PCA security and AE has one-time authenticity and one-time CCA security, then our compiler is able to compile a UC-secure PAKE to a UC-secure aPAKE, as shown in the following theorem.

**Theorem 1.** If KEM is a key encapsulation mechanism with OW-PCA security, AE is an authenticated encryption scheme with one-time authenticity and onetime CCA security,  $H_0, H_1, H_2, H_3, H_4$  work as random oracles, then the aPAKE scheme in Fig. 5 securely emulates  $\mathcal{F}_{apake}$ , hence achieving UC security in the  $\{\mathcal{F}_{pake}, \mathcal{F}_{RO}\}$ -hybrid model. More precisely, suppose there are at most N parties,  $\ell$  sessions and q random oracle queries, then there exists a simulator Sim s.t.

$$\begin{split} |\Pr\left[\mathbf{Real}_{\mathcal{Z},\mathcal{A}}\right] - \Pr\left[\mathbf{Ideal}_{\mathcal{Z},\mathsf{Sim}}\right]| \leq & N^2\ell \cdot \mathsf{Adv}_{\mathsf{KEM}}^{\mathsf{ow-pca}}(\mathcal{B}_{\mathsf{KEM}}) + \frac{q^2 + q + 1}{2^{\lambda}} \\ + & \ell \cdot \mathsf{Adv}_{\mathsf{AE}}^{\mathsf{ot-auth}}(\mathcal{B}_{\mathsf{AE}}) + \ell \cdot \mathsf{Adv}_{\mathsf{AE}}^{\mathsf{ot-cca}}(\mathcal{B}_{\mathsf{AE}}). \end{split}$$

PROOF. The main objective of the proof is constructing a PPT simulator Sim to simulate an indistinguishable view for the environment  $\mathcal{Z}$ . Sim is designed to have access to the ideal functionality  $\mathcal{F}_{apake}$  and interact with the environment  $\mathcal{Z}$ , thereby emulating the real-world aPAKE protocol interactions involving the adversary  $\mathcal{A}$ , the parties, and the environment  $\mathcal{Z}$ . It is important to note that Sim does not possess any password.

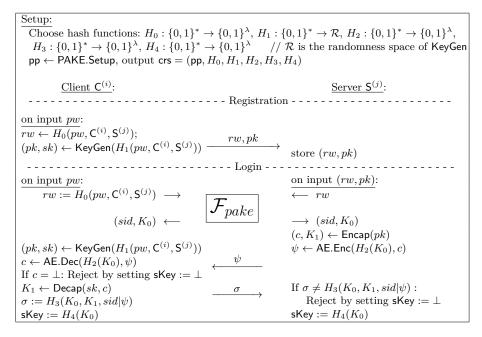


Fig. 5: Construction of UC-secure aPAKE from UC-secure PAKE with our compiler.

Let  $\operatorname{Real}_{\mathcal{Z},\mathcal{A}}$  represent the real-world experiment where the environment  $\mathcal{Z}$  interacts with the parties and adversary  $\mathcal{A}$  who can access ideal functionality  $\mathcal{F}_{pake}$  via Testpw and NewKey. Let  $\operatorname{Ideal}_{\mathcal{Z},\operatorname{Sim}}$  represents the ideal experiment where  $\mathcal{Z}$  interacts with "dummy" parties and simulator Sim. By  $\operatorname{Real}_{\mathcal{Z},\mathcal{A}} \Rightarrow 1$ , we mean  $\mathcal{Z}$  outputs 1 in  $\operatorname{Real}_{\mathcal{Z},\mathcal{A}}$ , and  $\operatorname{Ideal}_{\mathcal{Z},\operatorname{Sim}} \Rightarrow 1$  is similarly defined.

Our goal is to show that  $|\Pr[\operatorname{\mathbf{Real}}_{\mathcal{Z},\mathcal{A}} \Rightarrow 1] - \Pr[\operatorname{\mathbf{Ideal}}_{\mathcal{Z},\operatorname{Sim}} \Rightarrow 1]|$  is negligible by employing a series of games, denoted as Game  $G_0$ - $G_7$ . In this sequence,  $G_0$  corresponds to  $\operatorname{\mathbf{Real}}_{\mathcal{Z},\mathcal{A}}$ , while  $G_7$  corresponds to  $\operatorname{\mathbf{Ideal}}_{\mathcal{Z},\operatorname{Sim}}$ . We aim to show that these adjacent games are indistinguishable from the view of  $\mathcal{Z}$ . For simplicity, we write  $H_0(pw, \mathsf{C}^{(i)}, \mathsf{S}^{(j)})$  and  $H_1(pw, \mathsf{C}^{(i)}, \mathsf{S}^{(j)})$  as  $H_0(pw)$  and  $H_1(pw)$  in the security proof.

**Game G**<sub>0</sub>. This is the real experiment  $\operatorname{Real}_{\mathcal{Z},\mathcal{A}}$ . In this experiment,  $\mathcal{Z}$  initializes a password for each client-server pair, sees the interactions among clients, servers, ideal functionality  $\mathcal{F}_{pake}$  and adversary  $\mathcal{A}$ , and also obtains the corresponding session keys of protocol instances. During the execution,  $\mathcal{F}_{pake}$  may be invoked to create records like "(P, iid, Q, rw)" which we call *inner records* so as to distinguish them from the records created by  $\mathcal{F}_{apake}$ . Here  $\mathcal{A}$  may implement attacks like view, modify, insert, or drop messages over the network. In G<sub>0</sub>,  $H_0, H_1, H_2, H_3, H_4$  works as random oracles. Each party will do the following.

- For a server  $S^{(j)}$  on input (StorePWFile,  $C^{(i)}, S^{(j)}, pw$ ) from  $\mathcal{Z}$ , it computes  $rw := H_0(pw)$  and  $(pk, sk) \leftarrow \text{KeyGen}(H_1(pw))$  and then stores  $(C^{(i)}, S^{(j)}, rw, pk)$  locally.

- For a server  $S^{(j)}$  on input (StealPWFile,  $C^{(i)}, S^{(j)}$ ) from  $\mathcal{A}$ , it retrieves ( $C^{(i)}, S^{(j)}, rw, pk$ ) from local storage, and returns (rw, pk) to  $\mathcal{A}$ .
- For a client instance  $(C^{(i)}, iid)$  on input  $(NewClient, C^{(i)}, iid, S^{(j)}, pw)$  from  $\mathcal{Z}$ , it computes  $rw := H_0(pw)$  and issues " $(NewClient, C^{(i)}, iid, S^{(j)}, rw)$ " query to ideal functionality  $\mathcal{F}_{pake}$ . According to the specification of  $\mathcal{F}_{pake}$ , it will create a fresh inner record " $(NewClient, C^{(i)}, iid, S^{(j)}, rw)$ ", and send " $(NewClient, C^{(i)}, iid, S^{(j)})$ " to  $\mathcal{A}$ .

If  $\mathcal{A}$  issues "(NewKey,  $\mathsf{C}^{(i)}$ , *iid*, *sid*, Key<sup>\*</sup>)" to  $\mathcal{F}_{pake}$ , then the instance ( $\mathsf{C}^{(i)}$ , *iid*) may receive "(*sid*, Key =  $K_0$ )" from  $\mathcal{F}_{pake}$ .

- For a server instance  $(S^{(j)}, iid')$  on input (NewServer,  $S^{(j)}, iid', C^{(i)}$ ) from  $\mathcal{Z}$ , it retrieves  $(C^{(i)}, S^{(j)}, rw, pk)$  from its storage, and sends "(NewServer,  $S^{(j)}$ ,  $iid', C^{(i)}, rw$ )" to  $\mathcal{F}_{pake}$ . According to the specification of  $\mathcal{F}_{pake}$ , it will create a fresh inner record " $(S^{(j)}, iid', C^{(i)}, rw)$ ", and send "(NewServer,  $S^{(j)},$  $iid', C^{(i)}$ )" to  $\mathcal{A}$ .

If  $\mathcal{A}$  issues "(NewKey,  $\mathsf{S}^{(j)}$ , *iid'*, *sid*, Key<sup>\*</sup>)" to  $\mathcal{F}_{pake}$ , then the instance ( $\mathsf{S}^{(j)}$ , *iid'*) may receive "(*sid*, Key =  $K_0$ )" from  $\mathcal{F}_{pake}$ .

- $\mathcal{A}$  can access  $\mathcal{F}_{pake}$  via two interfaces (Testpw, P, iid, pw) and (NewKey,  $P, iid, sid, \text{Key}^*$ ).
  - Upon  $\mathcal{F}_{pake}$  receiving "(NewKey,  $P, iid, sid, Key^*$ )" from  $\mathcal{A}, \mathcal{F}_{pake}$  may create " $(sid, Key = K_0)$ " according to the specification in Fig. 3, mark the inner record "(P, iid, Q, rw)" as completed, and send " $(sid, Key = K_0)$ " to the instance "(P, iid)".
  - Upon  $\mathcal{F}_{pake}$  receiving "(Testpw, P, iid, rw')" query from  $\mathcal{A}$ , it checks whether  $rw' = H_0(pw)$ . If yes,  $\mathcal{F}_{pake}$  returns "correct guess" to  $\mathcal{A}$ . Otherwise,  $\mathcal{F}_{pake}$  returns "wrong guess" to  $\mathcal{A}$ . Meanwhile,  $\mathcal{F}_{pake}$  marks the inner record "(P, iid, Q, rw)" as compromised or interrupted accordingly (See Fig. 3).
- Upon a server instance  $(\mathsf{S}^{(j)}, iid')$  receiving message  $(sid, K_0)$  from  $\mathcal{F}_{pake}$ , it retrieves " $(\mathsf{C}^{(i)}, \mathsf{S}^{(j)}, rw, pk)$ " from its storage, and computes  $(c, K_1) \leftarrow \mathsf{Encap}(pk)$ . Then it computes  $\psi \leftarrow \mathsf{AE}.\mathsf{Enc}(H_2(K_0), c)$  and sends  $\psi$  to  $\mathcal{A}$ .
- Upon a client instance  $(C^{(i)}, iid)$  receiving message " $(sid, K_0)$ " from  $\mathcal{F}_{pake}$ and message  $\psi$  from  $\mathcal{A}$ , it first decrypts  $c \leftarrow \mathsf{AE}.\mathsf{Dec}(H_2(K_0), \psi)$ . If  $c = \bot$ , then it rejects and sends  $\bot$  to  $\mathcal{Z}$ . Otherwise, it computes  $(pk, sk) \leftarrow \mathsf{KeyGen}(H_1(pw))$  and decrypts  $K_1 \leftarrow \mathsf{Decap}(sk, c)$ . Finally, it computes  $\sigma := H_3(K_0, K_1, sid|\psi)$ , sends  $\sigma$  to  $\mathcal{A}$ , sets sKey :=  $H_4(K_0)$  and returns sKey to  $\mathcal{Z}$ .
- Upon a server instance  $(S^{(j)}, iid')$  receiving message  $\sigma$  from  $\mathcal{A}$ , if  $\sigma \neq H_3(K_0, K_1, sid|\psi)$ , then it rejects and sends  $\perp$  to  $\mathcal{Z}$ . Otherwise, it sets skey :=  $H_4(K_0)$  and returns skey to  $\mathcal{Z}$ .

We have

$$\Pr\left[\mathbf{Real}_{\mathcal{Z},\mathcal{A}} \Rightarrow 1\right] = \Pr\left[\mathsf{G}_0 \Rightarrow 1\right].$$

Game  $G_1$  (simulations for clients and servers with pw). In this game, we introduce a simulator Sim who *additional knows passwords* and has access

to the ideal functionality  $\mathcal{F}_{apake}$ . Now in Game  $G_1$ , the client and server become "dummy party" and directly forward their inputs to the ideal functionality  $\mathcal{F}_{apake}$  defined in Fig. 4. Then Sim simulates the behaviors of clients and servers with the help of pw as follows.

- For a dummy server  $S^{(j)}$  on input (StorePWFile,  $C^{(i)}, S^{(j)}, pw$ ) from Z, it directly sends this query to  $\mathcal{F}_{apake}$ . Then  $\mathcal{F}_{apake}$  sends (StorePWFile,  $C^{(i)}, S^{(j)}$ ) to Sim. Then Sim simulates the password file (rw, pk) with  $rw := H_0(pw)$ ,  $(pk, sk) \leftarrow \text{KeyGen}(H_1(pw))$ . Sim also stores a trapdoor record  $(C^{(i)}, S^{(j)}, rw, pk, sk, H_1(pw))$  in its local storage.
- For a dummy server  $S^{(j)}$  on input (StealPWFile,  $C^{(i)}, S^{(j)}$ ) from  $\mathcal{A}$ , Sim directly sends this query to  $\mathcal{F}_{apake}$ . Then  $\mathcal{F}_{apake}$  functions as described in Fig. 4 and sends (StealPWFile,  $C^{(i)}, S^{(j)}$ ) to Sim. Then Sim returns the password file (rw, pk) to  $\mathcal{A}$ .
- For a dummy client instance  $(C^{(i)}, iid)$  on input (NewClient,  $C^{(i)}, iid, S^{(j)}, pw$ ), it directly sends this query to  $\mathcal{F}_{apake}$ . Then  $\mathcal{F}_{apake}$  sends (NewClient,  $C^{(i)}, iid$ ,  $S^{(j)}$ ) to Sim and Sim simulates the behavior of the client instance ( $C^{(i)}, iid$ ) with the password pw, just like  $G_0$ .
- with the password pw, just like  $G_0$ . - For a dummy server instance  $(S^{(j)}, iid')$  on input (NewServer,  $S^{(j)}, iid, C^{(i)})$ , it directly sends this query to  $\mathcal{F}_{apake}$ . Then  $\mathcal{F}_{apake}$  sends (NewServer,  $S^{(j)}, iid'$ ,  $C^{(i)}$ ) to Sim and Sim simulates the behavior of the server instance  $(S^{(j)}, iid')$ with the PAKE password rw, just like  $G_0$ .
- For dummy client and server instances, the generations of  $\psi$ ,  $\sigma$  and sKey are all simulated by Sim with the password pw, just like  $G_0$ .

With the knowledge of *passwords*, the simulations of the behaviors of all clients and servers are perfect.

Moreover, Sim also simulates random oracles  $H_i$   $(i \in [0, 4])$  maintaining separate lists, namely  $\mathcal{L}_{H_i}$ . For a query x on  $H_i(\cdot)$ , if  $(x, y) \in \mathcal{L}_{H_i}$ , then Sim will return y as the reply. Otherwise, Sim will choose a random element y, record (x, y) in  $\mathcal{L}_{H_i}$ , and return y as the reply.

During the simulation, Sim additionally checks a bad event: if there exists two different random oracle queries to  $H_i$  such that  $H_i(pw) = H_i(pw')$ , then Sim will abort the game. By the ideal functionality of random oracles, Sim's simulations for oracles  $H_i$  are perfect except a collision occurs in the simulation of  $H_i$ . Suppose that the adversary issues q random oracle queries totally, by the union bound, we have

$$\left|\Pr\left[\mathsf{G}_1 \Rightarrow 1\right] - \Pr\left[\mathsf{G}_0 \Rightarrow 1\right]\right| \le \frac{q^2}{2^{\lambda}}.$$

The following games will change the simulations of Sim step by step in an indistinguishable way so that Sim can arrive at its final form in Fig. 6 and Fig. 7 in Appendix A, and accomplish the simulations in  $\mathbf{Ideal}_{\mathcal{Z},\mathsf{Sim}}$  without passwords pw.

Game  $G_2$  (simulation for ideal functionality  $\mathcal{F}_{pake}$  without pw). In  $G_2$ , simulator Sim will simulate the ideal functionality  $\mathcal{F}_{pake}$  itself, but without the

knowledge of pw. More precisely, Sim will maintain some inner records to simulate the output of  $\mathcal{F}_{pake}$  in the following way.

- Upon receiving (NewClient,  $C^{(i)}$ , iid,  $S^{(j)}$ ) from  $\mathcal{F}_{apake}$ : Sim sends (NewClient,  $C^{(i)}$ , iid,  $S^{(j)}$ ) to  $\mathcal{A}$ . Then it stores " $(C^{(i)}$ , iid,  $S^{(j)}$ ,?)" as an inner record and marks it as fresh.
- Upon receiving input (NewServer, S<sup>(j)</sup>, *iid'*, C<sup>(i)</sup>) from *F*<sub>apake</sub>: Sim sends (NewServer, S<sup>(j)</sup>, *iid'*, C<sup>(i)</sup>) to *A*. Then it stores "(S<sup>(j)</sup>, *iid'*, C<sup>(i)</sup>, ?)" as an inner record and marks it as fresh.
- Upon receiving a query (Testpw, P, iid, rw) from  $\mathcal{A}$ : If there exists a fresh inner record "(P, iid, Q, ?)", then do the following. 1. If there exists  $(pw, rw) \in \mathcal{L}_{H_0}$ , then Sim sends (Testpw, P, iid, pw) to
  - 1. If there exists  $(pw, rw) \in \mathcal{L}_{H_0}$ , then Sim sends (Testpw, P, *iid*, pw) to  $\mathcal{F}_{apake}$  and forwards  $\mathcal{F}_{apake}$ 's reply ("correct guess" or "wrong guess") to  $\mathcal{A}$ .
  - 2. If  $\mathcal{A}$  ever issued (StealPWFile,  $C^{(i)}, S^{(j)}$ ) query before and Sim returned (rw', pk') to  $\mathcal{A}$  with rw' = rw, and (P, iid) is an instance among the interaction of  $C^{(i)}$  and  $S^{(j)}$ , then Sim returns "correct guess" to  $\mathcal{A}$ .
  - 3. In other cases, return "wrong guess".
  - 4. If Sim returns "correct guess" to A, it also replaces "(P, iid, Q, ?)" with "(P, iid, Q, rw)" and marks it as a compromised inner record. Otherwise, it marks "(P, iid, Q, ?)" as an interrupted inner record.
- Upon receiving a query (NewKey, P, iid, sid, Key<sup>\*</sup>) from  $\mathcal{A}$ : The simulator replies the query just like  $\mathcal{F}_{pake}$ .
  - 1. If sid has been assigned to  $\hat{P}$ 's any other instance (P, iid'), return  $\perp$ .
  - 2. If there exists a **compromised** inner record "(P, iid, Q, rw)", then output  $(sid, \text{Key}^*)$  to P.
  - 3. If there exists a **fresh** inner record "(P, iid, Q, ?)" and a **completed** inner record "(Q, iid', P, ?)", "(sid, Key')" was sent to Q and (Q, iid', P, ?) was **fresh** at the time, then output "(sid, Key')" to P.
  - 4. In any other case, pick a new random key  $\mathsf{Key} \leftarrow \{0,1\}^{\lambda}$  and send " $(sid,\mathsf{Key})$ " to P.

Finally, mark the inner record " $(P, iid, Q, \cdot)$ " as completed.

It is easy to see the simulation of NewClient, NewServer, NewKey query is perfect. The only difference in  $G_1$  and  $G_2$  occurs in the simulation of Testpw query.

Note that in  $G_1$ , (Testpw, P, iid, rw) returns "correct guess" if and only if rw is the PAKE password used in the instance (P, iid), which is the case that  $rw = H_0(pw)$  for the input pw to party P. Therefore,  $G_2$  and  $G_1$  differs only when  $\mathcal{A}$  issues a (Testpw, P, iid, rw) query to  $\mathcal{F}_{pake}, rw = H_0(pw)$  but  $\mathcal{A}$  does not query  $H_0(pw)$ . By the ideal functionality of random oracle,  $H_0(pw)$  is uniformly distributed to  $\mathcal{A}$  if  $\mathcal{A}$  does not query it. So we have

$$\left|\Pr\left[\mathsf{G}_2 \Rightarrow 1\right] - \Pr\left[\mathsf{G}_1 \Rightarrow 1\right]\right| \le \frac{1}{2^{\lambda}}.$$

Game  $G_3$  (replace hash values of  $K_0$  with uniform ones unless  $\mathcal{A}$  implements a successful on-line active attacks on  $\mathcal{F}_{pake}$ ). We consider the

following three cases, where Case I and Case II cover  $\mathcal{A}$ 's successful on-line active attacks on  $\mathcal{F}_{pake}$ , and Case III covers the rest.

- **Case I.**  $\mathcal{A}$  implements a (successful) on-line attack on  $\mathcal{F}_{pake}$  with the correct password pw. That is,  $\mathcal{A}$  issues "(Testpw, P, iid, rw = H(pw))" query, and then Sim obtains "correct guess" from  $\mathcal{F}_{apake}$  for its query "(Testpw, P, iid, pw)" to  $\mathcal{F}_{apake}$ . In this case, Sim is able to extract the correct password pw.
- **Case II.**  $\mathcal{A}$  implements a (successful) on-line attack on  $\mathcal{F}_{pake}$  by impersonating a party with the stolen PAKE password rw. That is  $\mathcal{A}$  first issues a query (StealPWFile, P, Q), then issues "(Testpw, P, iid, rw)" or "(Testpw, Q, iid, rw)" query. In this case,  $\mathcal{A}$  has stolen the PAKE password rw and successfully implements an on-line impersonation attack.
- Case III. Neither Case I nor Case II occurs.

If Case I or Case II happens,  $G_3$  is the same as  $G_2$ . But if Case III happens in  $G_3$ , when  $\mathcal{A}$  issues a "(NewKey, P, *iid*, Key<sup>\*</sup>)" query resulting in  $K_0$ , then the hash values of  $H_2(K_0)$ ,  $H_3(K_0, K_1, c)$  and  $H_4(K_0)$  are replaced with independently and uniformly chosen elements, no matter whether  $\mathcal{A}$  has ever queried any of them or not.

It is easy to see that  $G_3$  is the same as  $G_2$  unless  $\mathcal{A}$  has ever queried  $H_2(K_0)$ ,  $H_3(K_0, K_1, c)$  or  $H_4(K_0)$  in Case III.

Note that Case III means that either there is no on-line attacks from  $\mathcal{A}$  or the on-line attack does not succeed. Upon  $\mathcal{A}$  issuing a "(NewKey, P, iid, Key<sup>\*</sup>)" query to  $\mathcal{F}_{pake}$  in Case III, then the resulting key  $K_0$  simulated by Sim is uniformly distributed to  $\mathcal{A}$  (according to the specification of the simulation of ideal functionality  $\mathcal{F}_{pake}$ , the session key  $K_0$  should be uniform). Suppose the adversary totally issues q random oracle queries, then  $\mathcal{A}$  ever issues hash query  $H_2(K_0), H_3(K_0, K_1, c)$  or  $H_4(K_0)$  with correct  $K_0$  with probability at most  $q/2^{\lambda}$ . So we have

$$\left|\Pr\left[\mathsf{G}_3 \Rightarrow 1\right] - \Pr\left[\mathsf{G}_2 \Rightarrow 1\right]\right| \le \frac{q}{2^{\lambda}}.$$

Now in Case III, the AE key  $H_2(K_0)$ , the authenticator  $\sigma = H_3(K_0, K_1, c)$ and the session key  $\mathsf{sKey} = H_4(K_0)$  will be uniformly distributed to  $\mathcal{A}$ . Jumping ahead, the uniform AE key  $H_2(K_0)$  in Case III paves the way for the security reduction to the security of AE in  $\mathsf{G}_4$  and  $\mathsf{G}_5$ .

Now in G<sub>3</sub>, Sim does not need pw to simulate the generation of PAKE session key  $K_0$ : upon  $\mathcal{A}$ 's (NewKey, P, iid, Key<sup>\*</sup>) query, Sim just sets  $K_0 :=$  Key<sup>\*</sup> in Case I and Case II, and can choose  $K_0$  uniformly in Case III. But Sim still needs rw to identify Case II and needs password pw to generate password file. Moreover, the generations of  $\psi$  and  $\sigma$  also needs pw:  $(pk, sk) \leftarrow \text{KeyGen}(H_1(pw)), (c, K_1) \leftarrow$  $\text{Encap}(pk), \psi \leftarrow \text{AE.Enc}(H_2(K_0), c), \text{ and } \sigma = H_3(K_0, K_1 = \text{Decap}(sk, c), sid|\psi).$ 

Game  $G_4$  (Simulation of generating server's message  $\psi$  without pw). In  $G_4$ , Sim is the same as in  $G_3$ , except for Sim's generation of  $\psi$  for the server instance  $(S^{(j)}, iid')$ . We describe Sim's simulations in the three cases (which are defined in  $G_3$ ) in  $G_4$ .

- If Case I occurs to  $(S^{(j)}, iid')$ , then Sim does not need to know pw beforehand. Instead, Sim can extract the true password pw of server  $S^{(j)}$  from  $\mathcal{F}_{apake}$ . Then Sim can use pw to generate  $(pk, sk) \leftarrow \text{KeyGen}(H_1(pw)), (c, K_1) \leftarrow \text{Encap}(pk)$  and  $\psi \leftarrow \text{AE.Enc}(H_2(K_0), c)$ , exactly like  $G_3$ .
- If Case II occurs to  $(\mathsf{S}^{(j)}, iid')$ , then Sim does not need the knowledge of pw to generate  $\psi$ . In this case, Sim directly retrieves pk from its trapdoor record  $(\mathsf{C}^{(i)}, \mathsf{S}^{(j)}, rw, pk, sk, r)$ , and then compute  $(c, K_1) \leftarrow \mathsf{Encap}(pk)$  and generates  $\psi \leftarrow \mathsf{AE}.\mathsf{Enc}(H_2(K_0), c)$ . Simulation of  $\psi$  is exactly the same as  $\mathsf{G}_3$ .
- If neither Case I nor Case II occurs to  $(S^{(j)}, iid')$ , then Sim does not need the knowledge of pw to generate  $\psi$  either. In this case, Sim directly retrieves pk from its trapdoor record  $(C^{(i)}, S^{(j)}, rw, pk, sk, r)$  and then computes  $(c, K_1) \leftarrow \mathsf{Encap}(pk)$  and  $\psi \leftarrow \mathsf{AE}.\mathsf{Enc}(H_2(K_0), 0)$ . Accordingly, when its partnered client instance  $(C^{(i)}, iid)$  receives this specific  $\psi$  (passive attack with  $\psi$ ), it directly uses  $K_1$  corresponding to  $\psi$  (for consistence) and computes  $\sigma := H_3(K_0, K_1, sid|\psi)$ . Recall that in  $\mathsf{G}_3, \psi \leftarrow \mathsf{AE}.\mathsf{Enc}(H_2(K_0), c)$ rather than  $\psi \leftarrow \mathsf{AE}.\mathsf{Enc}(H_2(K_0), 0)$ .

Finally, simulator Sim records  $(S^{(j)}, iid', K_1)$  in Case I and Case II and records  $(S^{(j)}, iid', \bot)$  in Case III.

The difference between  $G_3$  and  $G_4$  lies in the generation of  $\psi$  in Case III:  $\psi \leftarrow \mathsf{AE}.\mathsf{Enc}(H_2(K_0), c)$  in  $G_3$  but  $\psi \leftarrow \mathsf{AE}.\mathsf{Enc}(H_2(K_0), 0)$  in  $G_4$ . In Case III,  $H_2(K_0)$  is uniformly distributed and independent of  $\mathcal{A}$ 's view, as shown in  $G_3$ . According to the one-time IND-CCA security of  $\mathsf{AE}$  and hybrid arguments over the (at most)  $\ell$  ciphertexts of  $\mathsf{AE}$ , we have

$$|\Pr[\mathsf{G}_4 \Rightarrow 1] - \Pr[\mathsf{G}_3 \Rightarrow 1]| \le \ell \cdot \mathsf{Adv}_{\mathsf{AE}}^{\mathsf{ot-cca}}(\mathcal{B}_{\mathsf{AE}}).$$

Note that the reduction needs to query the decryption oracle once to simulate the message  $\sigma$  when it receives  $\psi$  generated by  $\mathcal{A}$ . This is why we need AK have one-time IND-CCA security.

Now in  $G_4$ , Sim only needs rw to distinguish Case II and pk to simulate the generation of  $\psi$  in Case II. Besides Sim also uses pk to generate  $c, K_1$  in Case II, III, and uses sk to generate  $\sigma$  in Case II, III. But it still needs pw to generate (rw, pk, sk).

Game  $G_5$  (Simulation of client's message  $\sigma$  and session key sKey without pw). In  $G_5$ , Sim is the same as in  $G_4$ , except for Sim's generation of  $\sigma$  and sKey for the client instance ( $C^{(i)}$ , *iid*) when receiving  $\psi$ . We describe Sim's simulations in the three cases in  $G_5$ .

- Case I occurs to  $(C^{(i)}, iid)$ :  $\mathcal{A}$  successfully guesses pw by issuing "(Testpw,  $C^{(i)}, iid, rw = H_0(pw)$ )" query to  $\mathcal{F}_{pake}$ . In this case, Sim can extract the true password pw from  $\mathcal{F}_{apake}$  and simulate the generation of  $\sigma$  in the same way as  $G_4$ . More precisely, Sim first decrypts  $c \leftarrow AE.Dec(H_2(K_0), \psi)$ . - If  $c = \bot$ , then Sim issues (Abort,  $C^{(i)}, iid$ ) query to  $\mathcal{F}_{apake}$ . As a result,  $\mathcal{F}_{apake}$  returns  $(\bot, \bot)$  to  $(C^{(i)}, iid)$  to reject the session. In this case the session is rejected in both  $G_4$  and  $G_5$ . – Otherwise, Sim generates  $(pk, sk) \leftarrow \text{KeyGen}(H_1(pw))$ , decrypts  $K_1 \leftarrow \text{Decap}(sk, c)$  and computes  $\sigma := H_3(K_0, K_1, sid|\psi)$ . Finally, Sim issues

(CorruptKey,  $C^{(i)}$ , iid,  $sid|\psi|\sigma$ ,  $H_4(K_0)$ ) query to  $\mathcal{F}_{apake}$  and  $\mathcal{F}_{apake}$  returns  $(sid|\psi|\sigma, sKey = H_4(K_0))$  to  $(C^{(i)}, iid)$ . In this case  $sKey = H_4(K_0)$  and  $\sigma = H_3(K_0, K_1, sid|\psi)$  in both  $G_4$  and  $G_5$ .

- Case II occurs to  $(C^{(i)}, iid)$ :  $\mathcal{A}$  must have stolen server's password file and then impersonates party  $S^{(j)}$ . In this case, Sim first decrypts  $c \leftarrow \mathsf{AE}.\mathsf{Dec}(H_2(K_0), \psi).$ 

- If  $c = \bot$ , then Sim issues (Abort,  $C^{(i)}$ , *iid*) query to  $\mathcal{F}_{apake}$ . As a result,  $\mathcal{F}_{apake}$  returns  $(\bot, \bot)$  to  $(C^{(i)}, iid)$  to reject the session. In this case the session is rejected in both  $G_4$  and  $G_5$ .

- If  $c \neq \bot$ , then Sim retrieves sk from its trapdoor record  $(\mathsf{C}^{(i)},\mathsf{S}^{(j)}, rw, pk, sk, r)$  to decrypt  $K_1 \leftarrow \mathsf{Decap}(sk, c)$  and computes  $\sigma := H_3(K_0, K_1, sid|\psi)$ . Then Sim issues (Impersonate,  $\mathsf{C}^{(i)}, iid$ ) query to  $\mathcal{F}_{apake}$ , which indicates that Sim impersonates  $\mathsf{S}^{(j)}$  to attack  $(\mathsf{C}^{(i)}, iid)$ . Finally, Sim issues (CorruptKey,  $\mathsf{C}^{(i)}$  $iid, sid|\psi|\sigma, H_4(K_0)$ ) query to  $\mathcal{F}_{apake}$  and then  $\mathcal{F}_{apake}$  must return  $(sid|\psi|\sigma, \mathsf{sKey} = H_4(K_0))$  to  $(\mathsf{C}^{(i)}, iid)$ . In this case the session key is  $\mathsf{sKey} = H_4(K_0)$  and  $\sigma = H_3(K_0, K_1, sid|\psi)$  in both  $\mathsf{G}_4$  and  $\mathsf{G}_5$ .

- Case III: neither Case I nor Case II occurs to  $(C^{(i)}, iid)$ . In this case,  $K_0, H_2(K_0), H_3(K_0, K_1, c)$  and  $H_4(K_0)$  are all simulated with uniform ones by Sim. We further consider the following two subcases according to passive or active attacks.

- **Passive Attack with**  $\psi$ : In this case,  $(C^{(i)}, iid)$  and  $(S^{(j)}, iid')$  must have shared the same PAKE session key  $K_0$  and  $\psi$  must be generated by Sim for some instance  $(S^{(j)}, iid')$ . Sim randomly chosen  $\sigma \leftarrow \{0, 1\}^{\lambda}$  and issues (FreshKey,  $C^{(i)}, iid, sid|\psi|\sigma)$  query to  $\mathcal{F}_{apake}$ . Then  $\mathcal{F}_{apake}$  returns a uniform session key sKey  $\leftarrow \{0, 1\}^{\lambda}$  to  $(C^{(i)}, iid)$ . Later if the server session  $(S^{(j)}, iid')$ receives the same  $\sigma$  later, Sim will issue (CopyKey,  $S^{(j)}, iid', sid|\psi|\sigma)$  query to  $\mathcal{F}_{apake}$  directly. In this case,  $(C^{(i)}, iid)$  and  $(S^{(j)}, iid')$  share a same uniform session key chosen by  $\mathcal{F}_{apake}$ .

- Active Attack with  $\psi$ : In this case  $\psi$  is not generated by Sim or instance  $(S^{(j)}, iid')$  and  $(C^{(i)}, iid)$  do not share a same PAKE session key. Sim issues (Abort,  $C^{(i)}, iid$ ) query to  $\mathcal{F}_{apake}$ . As a result,  $\mathcal{F}_{apake}$  returns  $(\bot, \bot)$  to  $(C^{(i)}, iid)$  to reject the session.

In both sub-cases, Sim does not need to retrieve pk to generate c via  $(c, K_1) \leftarrow \mathsf{Encap}(pk)$  for the server instance  $(\mathsf{S}^{(j)}, iid')$ , and it does not need to retrieve sk to decrypt c for client instance  $(\mathsf{C}^{(i)}, iid)$  any more.

If Case I or Case II occurs,  $\mathsf{G}_4$  and  $\mathsf{G}_5$  are the same, as analysed above. The difference lies in Case III.

Recall in  $G_4$ , if neither Case I nor Case II occurs, then  $K_0$  is uniform and independent of  $\mathcal{A}$ 's view. Consequently,  $H_3(K_0, K_1, sid|\psi)$ ,  $H_4(K_0)$ ,  $H_2(K_0)$  are all uniform to  $\mathcal{A}$  and independent of  $\mathcal{A}$ 's view. In the case of passive attack where  $\psi$  is generated by Sim, the client message  $\sigma := H_3(K_0, K_1, sid|\psi)$  and the client session key  $\mathsf{sKey} := H_4(K_0)$  are uniform to  $\mathcal{A}$ . In  $\mathsf{G}_5$ ,  $\sigma$  and  $\mathsf{sKey}$  are uniformly chosen. Therefore,  $\sigma$  and  $\mathsf{sKey}$  have the same distribution in  $\mathsf{G}_4$  and  $\mathsf{G}_5$ . In the case of active attack with  $\psi$ , Sim directly rejects  $\psi$  in  $\mathsf{G}_5$ . But in  $\mathsf{G}_4$ , Sim accepts if  $\psi$  is valid and rejects otherwise.  $\mathsf{G}_5$  and  $\mathsf{G}_4$  are the same unless the event  $\mathbf{Bad}_{\mathbf{Auth}}$  happens, where  $\mathbf{Bad}_{\mathbf{Auth}}$  is defined as

**Bad<sub>Auth</sub>**: Active attack with  $\psi$  results in AE.Dec $(H_2(K_0), \psi) \neq \bot$  in Case III.

With difference lemma, we know that  $|\Pr[\mathsf{G}_5 \Rightarrow 1] - \Pr[\mathsf{G}_4 \Rightarrow 1]| \leq \Pr[\mathbf{Bad}_{Auth}]$ . Recall that  $H_2(K_0)$  is uniformly distributed in Case III. Thanks to the authenticity of AE,  $\mathcal{A}$  only has negligible probability of generating a valid ciphertext  $\psi$  without the knowledge of  $H_2(K_0)$ .

Hence,  $\psi$  will always be rejected by  $(C^{(i)}, iid)$  except with a negligible probability. Given at most  $\ell$  sessions, we know that  $\Pr[\mathbf{Bad}_{\mathbf{Auth}}] \leq \ell \cdot \mathsf{Adv}_{\mathsf{AE}}^{\mathsf{ot-auth}}(\mathcal{B}_{\mathsf{AE}})$ . Consequently, we have

$$\left|\Pr\left[\mathsf{G}_5 \Rightarrow 1\right] - \Pr\left[\mathsf{G}_4 \Rightarrow 1\right]\right| \le \ell \cdot \mathsf{Adv}_{\mathsf{AE}}^{\mathsf{ot-auth}}(\mathcal{B}_{\mathsf{AE}}).$$

Note that  $\mathcal{A}$  may additionally see a valid ciphertext  $\psi$  generated by Sim. This is why we need a one-time secure authenticity AE scheme.

Now in  $G_5$ , Sim only needs rw to distinguish Case II, needs pk to simulate the generation of  $\psi$  for server instances in Case II, and needs sk to decrypt c so as to compute  $\sigma$  for client instances in Case II. But it still needs pw to generate (rw, pk, sk).

Game  $G_6$  (simulation for password file without pw). In  $G_6$ , Sim behaves the same as  $G_5$  except for the simulation of generating the password file (rw, pk).

Recall that in  $G_5$ , Sim uses password pw to generate the password file (rw, pk)upon  $\mathcal{A}$ 's StorePWFile query, but reveals the file to  $\mathcal{A}$  upon  $\mathcal{A}$ 's StealPWFile query. Sim also generates the trapdoor record along with the file but only uses the record for Case II in which StealPWFile must have happened. This fact suggests that Sim can delay the generation of password file (rw, pk) and the trapdoor record  $(C^{(i)}, S^{(j)}, rw, pk, sk, H_1(pw))$  until StealPWFile query. This is exactly Sim does without pw in  $G_6$ , but with the help of re-programming technique of ROs.

In  $G_6$ , Sim will keep the password file and the trapdoor record empty until StealPWFile query from  $\mathcal{A}$ . We consider three phases of the game.

- **Before receiving** (StealPWFile,  $C^{(i)}, S^{(j)}$ ) from  $\mathcal{A}$ : In this phase, the simulations by Sim is exactly the same as that in  $G_5$ . Besides, Sim also does the following. For any random oracle query to  $H_0(x)$  or  $H_1(x)$  from  $\mathcal{A}$ , Sim will also issue a query (OfflineTestPW,  $C^{(i)}, S^{(j)}, x$ ) to  $\mathcal{F}_{apake}$  and  $\mathcal{F}_{apake}$  will store an offline-guess record.

Recall that only Case I or Case III happens in this phase. But neither pw nor the trapdoor record is needed by Sim for Case I and Case III in G<sub>5</sub>. So the simulation without pw in G<sub>6</sub> is sound in this phase.

- When receiving (StealPWFile,  $C^{(i)}, S^{(j)}$ ) from  $\mathcal{A}$ : It must happen that  $\mathcal{A}$  has issued a StealPWFile query to a dummy server  $S^{(j)}$  and then Sim issues a StealPWFile query to  $\mathcal{F}_{apake}$ . According to the specification of  $\mathcal{F}_{apake}$  in Fig. 4,  $\mathcal{F}_{apake}$  sends (StealPWFile,  $C^{(i)}, S^{(j)}$ ) to Sim.

Upon the output (StealPWFile,  $C^{(i)}, S^{(j)}$ ) from  $\mathcal{F}_{apake}$ ,

(1) If Sim ever issued a (OfflineTestPW,  $C^{(i)}, S^{(j)}, x$ ) query before such that  $x = pw, \mathcal{F}_{apake}$  must have additionally output pw and "correct guess" to Sim. In this case, Sim obtains the correct password pw, and then it can invoke  $(pk, sk) \leftarrow \text{KeyGen}(H_1(pw))$ , set  $rw := H_0(pw)$ , return (rw, pk) to  $\mathcal{A}$ , and set the trapdoor record as  $(C^{(i)}, S^{(j)}, rw, pk, sk, H_1(pw))$ . The simulations of password file and trapdoor record are exactly like  $G_5$ .

(2) Otherwise, Sim randomly samples rw ←s {0,1}<sup>λ</sup> and r ←s R, invokes (pk, sk) ← KeyGen(r), returns (rw, pk) to A, and stores record (C<sup>(i)</sup>, S<sup>(j)</sup>, rw, pk, sk, r). In this case, A did not ever query H<sub>0</sub>(pw) or H<sub>1</sub>(pw), so these hash values are uniform to A. Though Sim does not know the value of pw, it implicitly set H<sub>0</sub>(pw) := rw and H<sub>1</sub>(pw) = r. Therefore, in this case, the simulations of password file and trapdoor record are exactly the same from A's view no matter in in G<sub>6</sub> or G<sub>5</sub>.
After receiving (StealPWFile, C<sup>(i)</sup>, S<sup>(j)</sup>) from A: In this phase, Sim will

- After receiving (StealPWFile,  $C^{(i)}$ ,  $S^{(j)}$ ) from  $\mathcal{A}$ : In this phase, Sim will use the trapdoor record for the simulations, exactly like in  $G_5$ . Besides, Sim also keeps an eye on random oracle queries: For each new random oracle query for  $H_0(x)$  or  $H_1(x)$ , Sim will issue a query (OfflineTestPW,  $C^{(i)}$ ,  $S^{(j)}$ , x) to  $\mathcal{F}_{apake}$  and check the reply. If  $\mathcal{F}_{apake}$  returns "correct guess", Sim will retrieve the record ( $C^{(i)}$ ,  $S^{(j)}$ , rw, pk, sk, r) and  $reprogram H_0(x = pw) := rw$ and  $H_1(x = pw) := r$  by storing (x, rw) in list  $\mathcal{L}_{H_0}$  and (x, r) in list  $\mathcal{L}_{H_1}$ . As long as  $\mathcal{A}$  issues oracle queries on pw, Sim will detect it and obtains the correct password pw. In this way, Sim keeps the consistence between pwand the trapdoor record. Even if  $\mathcal{A}$ 's offline-attack succeeds, Sim still give a perfect simulation for  $\mathcal{A}$ , just like  $G_5$ .

Due to the simulation strategy and reprogramming technique, the distribution of trapdoor record  $(C^{(i)}, S^{(j)}, rw, pk, sk, r = H_1(pw))$  in  $G_6$  and  $G_5$  are exactly the same. Therefore, we have

$$\Pr\left[\mathsf{G}_6 \Rightarrow 1\right] = \Pr\left[\mathsf{G}_5 \Rightarrow 1\right].$$

Game  $G_7$  (Simulation of dealing with  $\sigma$  for server instances without pw). In  $G_7$ , Sim is the same as in  $G_6$ , except for the simulation of the server instance  $(S^{(j)}, iid')$  when receiving  $\sigma$ . We still consider Sim's simulations in the three cases in  $G_7$ .

First, Sim retrieves record  $(S^{(j)}, iid', K_1)$  (that was stored when  $\psi$  is simulated for  $(S^{(j)}, iid')$ ) and the corresponding PAKE key  $K_0$ .

**Case I occurs to**  $(S^{(j)}, iid')$ . If  $\sigma \neq H_3(K_0, K_1, sid|\psi)$ , then Sim sends (Abort,  $S^{(j)}, iid')$  to  $\mathcal{F}_{apake}$ . As a result,  $\mathcal{F}_{apake}$  returns  $(\bot, \bot)$  to  $(S^{(j)}, iid')$  to reject the session. If  $\sigma = H_3(K_0, K_1, sid|\psi)$ , then Sim sends (CorruptKey,  $S^{(j)}, iid'$ ,  $sid|\psi|\sigma, H_4(K_0)$ ) to  $\mathcal{F}_{apake}$ . Then  $\mathcal{F}_{apake}$  returns  $H_4(K_0)$  to  $(S^{(j)}, iid')$ . Recall in  $G_6$ , skey  $= \bot$  if  $\sigma$  is invalid and skey  $= H_4(K_0)$  if  $\sigma$  is valid. Therefore,  $G_6$  and  $G_7$  are the same in this case.

**Case II occurs to**  $(S^{(j)}, iid')$ . If  $\sigma \neq H_3(K_0, K_1, sid|\psi)$  or  $\sigma = H_3(K_0, K_1, sid|\psi)$ but  $\mathcal{F}_{apake}$  did not return "correct guess" to any of Sim's (OfflineTestPW,

 $C^{(i)}, S^{(j)}, pw'$  queries, then Sim sends (Abort,  $S^{(j)}, iid'$ ) to  $\mathcal{F}_{apake}$ . As a result,  $\mathcal{F}_{apake}$  returns  $(\perp, \perp)$  to  $(S^{(j)}, iid')$  to reject the session.

If  $\sigma = \dot{H}_3(K_0, K_1, sid|\psi)$  and  $\mathcal{F}_{apake}$  returned "correct guess" to one of Sim's (OfflineTestPW,  $C^{(i)}, S^{(j)}, pw'$ ) queries, then Sim sends (CorruptKey,  $S^{(j)}, iid'$ ,  $sid|\psi|\sigma, H_4(K_0)$ ) to  $\mathcal{F}_{apake}$ . Accordingly  $\mathcal{F}_{apake}$  returns  $(sid|\psi|\sigma, sKey := H_4(K_0))$  to  $(S^{(j)}, iid')$ .

Recall in  $G_6$ , as long as Case II occurs, the simulator will set the session key sKey :=  $H_4(K_0)$  if  $\sigma = H_3(K_0, K_1, sid|\psi)$ , and set sKey :=  $\bot$  if  $\sigma \neq H_3(K_0, K_1, sid|\psi)$ .

**Case III occurs to**  $(S^{(j)}, iid')$ . We further consider whether  $\sigma$  is from  $\mathcal{A}$ ' passive attack or active attack.

- Passive Attack with  $\sigma$ : In this case, there must exist some instance  $(C^{(i)}, iid)$  which has agreed PAKE key  $K_0$  with  $(S^{(j)}, iid')$ , and  $\sigma$  must be generated by Sim for  $(C^{(i)}, iid)$ . Moreover, Sim must also have issued (FreshKey,  $C^{(i)}, iid, sid|\psi|\sigma$ ) query to  $\mathcal{F}_{apake}$  and  $\mathcal{F}_{apake}$  returns a uniform session key sKey to  $(C^{(i)}, iid)$ . Now Sim issues (CopyKey,  $S^{(j)}, iid', sid|\psi|\sigma$ ) query to  $\mathcal{F}_{apake}$  directly. In this case,  $(C^{(i)}, iid)$  and  $(S^{(j)}, iid')$  share a same uniform session key sKey chosen by  $\mathcal{F}_{apake}$  and the session key sKey is simulated with the help of  $\mathcal{F}_{apake}$ , without the knowledge of pw or the trapdoor record, just like  $G_6$ .

- Active Attack with  $\psi$ : Sim sends (Abort,  $S^{(j)}$ , *iid'*) to  $\mathcal{F}_{apake}$ , and accordingly  $\mathcal{F}_{apake}$  returns  $(\bot, \mathsf{sKey} := \bot)$  to  $(S^{(j)}, iid')$  to reject the session. Recall that in Case III of  $\mathsf{G}_6$ ,  $H_4(K_0, K_1, sid|\psi)$  is uniformly distributed and independent of  $\mathcal{A}$ 's view, the simulator will reject the session by setting  $\mathsf{sKey} := \bot$  except with negligible probability.

Therefore,  $\mathsf{G}_6$  and  $\mathsf{G}_7$  are the same in Case III except with negligible probability.

According to the above analyses,  $\mathsf{G}_7$  and  $\mathsf{G}_6$  are the same except a bad event **Bad** happens, where

**Bad:** Case II occurs to some  $(S^{(j)}, iid')$ ,  $\sigma = H_3(K_0, K_1, sid|\psi)$ , but until then none of the Sim's (OfflineTestPW,  $C^{(i)}, S^{(j)}, pw'$ ) queries results in "correct guess".

With difference lemma, we know that  $|\Pr[\mathsf{G}_7 \Rightarrow 1] - \Pr[\mathsf{G}_6 \Rightarrow 1]| \leq \Pr[\mathbf{Bad}].$ Next we show a reduction algorithm  $\mathcal{B}_{\mathsf{KEM}}$  and prove  $\Pr[\mathbf{Bad}] \leq N^2 \ell \cdot \mathsf{Adv}_{\mathsf{KEM}}^{\mathsf{ow-pca}}(\mathcal{B}_{\mathsf{KEM}}).$ 

 $\mathcal{B}_{\mathsf{KEM}}$  obtains a public key  $pk^*$ , a key encapsulation  $c^*$ , and has access to oracle  $\mathsf{Check}(\cdot, \cdot)$  which on input (c, K) returns 1 iff  $\mathsf{Decap}(sk^*, c) = K$ .  $\mathcal{B}_{\mathsf{KEM}}$  aims to find  $K^*$  s.t.  $\mathsf{Decap}(sk^*, c^*) = K^*$ .

In the reduction,  $\mathcal{B}_{\mathsf{KEM}}$  plays the role of the simulator Sim in  $\mathsf{G}_7$ . It first randomly choose  $(\mathsf{C}^{(*)},\mathsf{S}^{(*)},iid') \leftarrow_{\$} [N] \times [N] \times [\ell]$ .  $\mathcal{B}_{\mathsf{KEM}}$  sets  $(\mathsf{S}^{(*)},iid')$  as the target instance. Suppose that  $(\mathsf{C}^{(*)},iid)$  is the partnered instance.  $\mathcal{B}_{\mathsf{KEM}}$  will detect whether **Bad** happen on  $(\mathsf{S}^{(*)},iid')$ .

- For any other instances,  $\mathcal{B}_{\mathsf{KEM}}$  behaves just like Sim does in  $G_7$ .
- For the instances  $(C^{(*)}, iid)$  and  $(S^{(*)}, iid')$ ,  $\mathcal{B}_{KEM}$  does the simulations as follows.
  - Before receiving (StealPWFile,  $C^{(*)}$ ,  $S^{(*)}$ ) from  $\mathcal{A}$ :  $\mathcal{B}_{KEM}$  behaves just like Sim does in  $G_7$ .
  - Upon receiving (StealPWFile,  $C^{(*)}, S^{(*)}$ ) from  $\mathcal{A}$ :  $\mathcal{B}_{KEM}$  issues a StealPWFile query to  $\mathcal{F}_{apake}$ . If  $\mathcal{F}_{apake}$  replies with pw and "correct guess", then **Bad** does not happen on  $(S^{(*)}, iid')$ , and  $\mathcal{B}_{KEM}$  aborts the game. Otherwise,  $\mathcal{B}_{KEM}$  randomly samples  $rw \leftarrow_{s} \{0, 1\}^{\lambda}$ , sets the trapdoor record as  $(C^{(*)}, S^{(*)}, rw, pk^*, sk = ?, r = ?)$ , and returns the password file  $(rw, pk^*)$  to  $\mathcal{A}$ .
  - After receiving (StealPWFile,  $C^{(*)}, S^{(*)}$ ) from  $\mathcal{A}$ : During this phase, for any offline attack from  $\mathcal{A}$ , if the corresponding (OfflineTestPW,  $C^{(*)}, S^{(*)}$ , pw') query to  $\mathcal{F}_{apake}$  results in "correct guess", then **Bad** does not happen on ( $S^{(*)}, iid'$ ) and  $\mathcal{B}_{KEM}$  aborts the game.

For the session between instances  $(C^{(*)}, iid)$  and  $(S^{(*)}, iid')$ ,  $\mathcal{B}_{KEM}$  first simulates the generation of PAKE key  $K_0$  without pw and trapdoor record, just like Sim. If Case II does not happen, then **Bad** does not happen on  $(S^{(*)}, iid')$  and  $\mathcal{B}_{KEM}$  aborts the game.

Next, for server instance  $(S^{(*)}, iid')$ ,  $\mathcal{B}_{\mathsf{KEM}}$  can simulate the generation of  $\psi$ ,  $\mathcal{B}_{\mathsf{KEM}}$  invokes  $\psi \leftarrow \mathsf{AE}.\mathsf{Enc}(H_2(K_0), c^*)$ . Since  $c^*$  is an encapsulation under  $pk^*$ , we know  $\mathcal{B}_{\mathsf{KEM}}$ 's simulation is perfect, just like Sim.

For client instance  $(C^{(*)}, iid)$  to deal with  $\psi'$ , recall that Sim may decrypt  $\psi'$  with  $sk^*$  to generate  $K'_1$  and then  $\sigma$ , but  $\mathcal{B}_{\mathsf{KEM}}$  has no  $sk^*$ at all. To deal with this problem,  $\mathcal{B}_{\mathsf{KEM}}$  resorts to ROs and the reprogramming techniques: upon  $(\mathsf{C}^{(*)}, iid)$  receiving  $\psi'$ ,  $\mathcal{B}_{\mathsf{KEM}}$  invokes  $c \leftarrow \mathsf{AE}.\mathsf{Dec}(H_2(K_0),\psi')$ . If  $c = \bot$ ,  $\mathcal{B}_{\mathsf{KEM}}$  behaves just like Sim (no  $sk^*$ involved). If  $c \neq \perp$ , for all hash queries  $H_3(K_0, K'_1, sid|\psi')$ ,  $\mathcal{B}_{\mathsf{KEM}}$  first checks whether there exists  $K'_1$  such that  $\mathsf{Check}(c, K'_1) = 1$ . If yes, set  $\sigma := H_3(K_0, K'_1, sid|\psi')$ . Otherwise randomly choose  $\sigma \leftarrow \{0, 1\}^{\lambda}$ , and set  $H_3(K_0, K'_1 =?, sid|\psi') := \sigma$  with ? denoting the undermined value of  $K'_1$ . It then returns  $\sigma$  to  $\mathcal{A}$  and returns  $\mathsf{sKey} := H_2(K_0)$  as the session key. If later  $\mathcal{A}$  issues any new query  $H_3(K_0, K'_1, sid|\psi'), \mathcal{B}_{\mathsf{KEM}}$  checks whether  $\mathsf{Check}(c, K'_1) = 1.$  If yes,  $\mathcal{B}_{\mathsf{KEM}}$  re-programme  $H_3(K_0, K'_1, sid|\psi') := \sigma.$ Upon  $(S^{(*)}, iid')$  receiving  $\sigma'$ . If there is no  $H_3$  query such that  $\sigma' =$  $H_3(K_0, K'_1, sid|\psi)$ , then **Bad** does not happen on  $(\mathsf{S}^{(*)}, iid')$  since  $\sigma'$  is hardly valid due to the uniformity of RO, and then  $\mathcal{B}_{KEM}$  aborts the game. Otherwise, find  $\mathcal{A}$ 's hash query such that  $\sigma' = H_3(K_0, K'_1, sid|\psi)$ ,  $\mathcal{B}_{\mathsf{KEM}}$  checks whether  $\mathsf{Check}(c, K'_1) = 1$ . If no, then  $K'_1 \neq K^*_1 := \mathsf{Decap}(sk^*)$ c) so  $\sigma' \neq H_3(K_0, K_1^*, sid|\psi)$ . Thus **Bad** does not happen on  $(\mathsf{S}^{(*)}, iid')$ and  $\mathcal{B}_{\mathsf{KEM}}$  aborts the game. If yes,  $\mathsf{Check}(c, K'_1) = 1$  implies  $K'_1 = K^*_1 =$  $\mathsf{Decap}(sk^*, c)$ . Now **Bad** happens,  $\mathcal{B}_{\mathsf{KEM}}$  just replies this  $K'_1$  as it answer to its OW-PCA challenger.

The above description and analysis shows that  $\mathcal{B}_{KEM}$  presents a perfect simulation like Sim. As long as **Bad** happens on  $(S^{(*)}, iid')$ ,  $\mathcal{B}_{KEM}$  wins in its OW-PCA

experiment. Consequently, we have

$$\mathsf{Adv}_{\mathsf{KEM}}^{\mathsf{ow-pca}}(\mathcal{B}_{\mathsf{KEM}}) = \Pr\left[\mathbf{Bad} \text{ on } (\mathsf{S}^{(*)}, iid')\right] = \frac{1}{N^2 \ell} \cdot \Pr\left[\mathbf{Bad}\right].$$

So,

$$|\Pr[\mathsf{G}_7 \Rightarrow 1] - \Pr[\mathsf{G}_6 \Rightarrow 1]| \leq \Pr[\mathbf{Bad}] = N^2 \ell \cdot \mathsf{Adv}_{\mathsf{KEM}}^{\mathsf{ow-pca}}(\mathcal{B}_{\mathsf{KEM}}).$$
  
Finally, by combining all the statements across  $\mathsf{G}_0\text{-}\mathsf{G}_7$ , we get

$$|\operatorname{Dr}[\operatorname{Dras}]| = \ln |\operatorname{Dr}[\operatorname{Ldes}]| = |\operatorname{Ldes}| =$$

$$\begin{aligned} |\Pr[\operatorname{\mathbf{Real}}_{\mathcal{Z},\mathcal{A}}] - \Pr[\operatorname{\mathbf{Ideal}}_{\mathcal{Z},\operatorname{Sim}}]| &\leq N^2 \ell \cdot \operatorname{\mathsf{Adv}}_{\operatorname{\mathsf{KEM}}}^{\operatorname{\mathsf{out-pta}}}(\mathcal{B}_{\operatorname{\mathsf{KEM}}}) + \frac{1 - 1}{2^{\lambda}} \\ &+ \ell \cdot \operatorname{\mathsf{Adv}}_{\operatorname{\mathsf{AE}}}^{\operatorname{ot-auth}}(\mathcal{B}_{\operatorname{\mathsf{AE}}}) + \ell \cdot \operatorname{\mathsf{Adv}}_{\operatorname{\mathsf{AE}}}^{\operatorname{ot-cta}}(\mathcal{B}_{\operatorname{\mathsf{AE}}}). \end{aligned}$$

Remark 2 (Tightly secure aPAKE compiler.). Note that in the security proof, the security loss is due to the guessing strategy in the reduction between  $G_7$ and  $G_6$ , which relies on the OW-PCA security of the KEM scheme. By imposing stronger security on KEM, it is possible to make the reduction a tight one. For example, Pan et. al. [26] proposed the OW-ChCCA security for KEM and presented instantiation of such a KEM with tight OW-ChCCA security based on the (Matrix) DDH assumption. The OW-ChCCA security considers a multi-user setting, where besides the check oracle, the adversary adaptively corrupt users to obtain their secret keys, gets multiple challenge ciphertext encapsulations  $\{c_j\}$ , adaptively reveals some ciphertexts  $\{c'_i\} \subseteq \{c_j\}$  to obtain encapsulation keys, and adaptively obtains decryption results for  $\{c'_k\}$  such that  $\{c_j\} \cap \{c'_k\} = \emptyset$ , and it requires that it is still hard for such an adversary to guess correctly an encapsulation key for any unrevealed ciphertext under public keys of uncorrupted users.

**Theorem 2.** Under the same condition as in Theorem 1, if KEM is replaced with an OW-ChCCA secure one and AE is an information-theoretical AE scheme with one-time authenticity and one-time CCA security, then we have

$$\left|\Pr\left[\mathbf{Real}_{\mathcal{Z},\mathcal{A}}\right] - \Pr\left[\mathbf{Ideal}_{\mathcal{Z},\mathsf{Sim}}\right]\right| \le \mathsf{Adv}_{\mathsf{KEM}}^{(N^2,\ell)-\mathsf{ChCCA}}(\mathcal{B}_{\mathsf{KEM}}) + \frac{2\ell + q^2 + q + 1}{2^{\lambda}}.$$

The security proof of Theorem 2 is given in Appendix B. In Appendix B, we recall the formal definition of OW-ChCCA security for KEM. Then we prove that our compiler is tightness-preserving when equipped with such a OW-ChCCA secure KEM. In Fig.10, we review the specific tightly OW-ChCCA secure KEM based on the Matrix DDH assumption, which was proposed in [26].

### 4 Instantiations of aPAKE from Our Compiler and PAKE

Our aPAKE compiler needs an OW-PCA secure KEM scheme and an AE scheme with one-time authenticity and one-time CCA security. A good candidate for AE is the canonical information-theoretic construction. Instantiation of one-time secure AE. For one-time secure AE, we present a concrete information-theoretically secure AE scheme  $AE_{it} = (AE.Enc, AE.Dec)$ from one-time pad and one-time MAC, using the Encrypt-then-MAC approach. Here the key space is  $\{0,1\}^{3\lambda}$ , the message space is  $\{0,1\}^{\lambda}$ , and the ciphertext space is  $\{0,1\}^{2\lambda}$ . All operations are over field  $\mathbb{F}_{2\lambda}$ .

- $\mathsf{AE}.\mathsf{Enc}(k,m)$  : Parse  $k := (k_1, k_2, k_3) \in \mathbb{F}_{2^{\lambda}} \times \mathbb{F}_{2^{\lambda}} \times \mathbb{F}_{2^{\lambda}}$  and  $m \in \mathbb{F}_{2^{\lambda}}$ . Compute  $c_1 := k_1 + m$  and  $c_2 = k_2 \times c_1 + k_3$ .
- $\mathsf{AE}.\mathsf{Dec}(k,c)$ : Parse  $k := (k_1, k_2, k_3) \in \mathbb{F}_{2^{\lambda}} \times \mathbb{F}_{2^{\lambda}} \times \mathbb{F}_{2^{\lambda}}$  and  $c = (c_1, c_2)$ . If  $c_2 \neq k_2 \times c_1 + k_3$ : return  $\perp$ . Otherwise return  $c_1 k_1$ .

**Lemma 1.** For the above AE, we have

$$\mathsf{Adv}_{\mathsf{AF}}^{\mathsf{ot-auth}}(\mathcal{A}) \leq 1/2^{\lambda}, \quad \mathsf{Adv}_{\mathsf{AF}}^{\mathsf{ot-cca}}(\mathcal{A}) \leq 1/2^{\lambda}.$$

for any (even all-powerful) adversaries.

The security proof of Lemma 1 is shown in Appendix C.

The OW-PCA security is a security notion weaker the CCA security, which admits flexible choices for the underling KEM in our compiler. Next we show how to instantiate our compiler according to the PAKE scheme so as the resulting aPAKE scheme enjoying good features.

#### 4.1 Most Efficient aPAKE from Lattice

Recall that there exists efficient UC-secure PAKE protocols [29,2,20] from lattice, where the PAKE protocol in [2,20] is based on Kyber [7] and that in [29] is based on Saber [10]. Kyber [7] is the NIST PQC winner for KEM, and its CCA security is based on the module-LWE assumption [21], so we choose the Kyber-based UC-secure PAKE scheme [2].

Now we also take Kyber (whose CCA security naturally implies OW-PCA security) as the KEM in our compiler. Then together with the information-theoretically secure  $AE_{it}$ , we obtain a Kyber-based aPAKE scheme (see Fig. 9 in Appendix E for a more detailed description of the scheme).

Note that the second to last round of our compiler can be merged in the last round of PAKE, resulting in a 3-round Kyber-based aPAKE scheme with UC-security.

**Comparison to other lattice-based aPAKEs.** Up to now, the only approach to lattice-based UC-secure aPAKE is via the signature-aided compiler proposed in [15]. However, signature schemes from lattice, like Dilithium or Falcon, are far less efficient than their KEM counterpart like Kyber. We compare our Kyber-based compiler to the Dilithium-based Compiler in [15] and the Falcon-based Compiler in [15] in terms of the computing and communication efficiency in Table 1.

The comparison in Table 1 suggests that our Kyber-based compiler is the most efficient one, and hence the resulting Kyber-based aPAKE scheme (=Kyber-based compiler + Kyber-based PAKE) is the *most efficient* aPAKE scheme with UC-security from lattice up to now.

**Corollary 1.** Under the same condition as in Theorem 1, suppose that KEM is instantiated with the CCA secure KEM scheme Kyber [7] and AE is an information-theoretical AE scheme with one-time authenticity and one-time CCA security in our compiler. If the underlying PAKE is instantiated with the UC-secure Kyberbased PAKE protocol in [2], then the resulting aPAKE has UC-security s.t.

 $\left|\Pr\left[\mathbf{Real}_{\mathcal{Z},\mathcal{A}}\right] - \Pr\left[\mathbf{Ideal}_{\mathcal{Z},\mathsf{Sim}}\right]\right| \leq (5q + 2q\ell + 2N^2\ell) \cdot \mathsf{Adv}_{k+1,k,\chi}^{\mathsf{mlwe}}(\mathcal{A}) + 2^{-\Omega(\lambda)},$ 

where  $\operatorname{Adv}_{k+1,k,\chi}^{\mathsf{mlwe}}(\mathcal{A})$  is the advantage function for the Module-LWE problem [21].

#### 4.2 Tightly Secure aPAKE Scheme from Matrix DDH

For the underlying PAKE protocol, there exist tightly UC-secure PAKE protocols from the CDH assumption [22,27]. Accordingly, our compiler also has tightly secure OW-ChCCA secure KEM [26] from the (Matrix) DDH assumption as candidate.

Now we take the MDDH-based KEM [26] with tight OW-ChCCA security as the KEM in our compiler. Then together with the information-theoretically secure  $AE_{it}$ , our compiler can compile the CDH-based tightly UC-secure PAKE scheme to a MDDH-based aPAKE scheme, which serves as the *first tightly UC-secure* aPAKE scheme up to now (See Fig. 9 in Appendix E for the tightly UC-secure aPAKE scheme).

**Corollary 2.** Under the same condition as in Theorem 2, suppose that KEM is instantiated with the tightly OW-ChCCA secure MDDH-based KEM in [26] and AE is an information-theoretical AE scheme with one-time authenticity and one-time CCA security in our compiler. If the underlying PAKE is instantiated with the tightly UC-secure CDH-based PAKE protocol in [22], then the resulting aPAKE has tight UC-security such that

 $\left|\Pr\left[\mathbf{Real}_{\mathcal{Z},\mathcal{A}}\right] - \Pr\left[\mathbf{Ideal}_{\mathcal{Z},\mathsf{Sim}}\right]\right| \le 12 \cdot \mathsf{Adv}_{\mathsf{MDDH}}(\mathcal{A}) + 2 \cdot \mathsf{Adv}_{\mathsf{CDH}}(\mathcal{A}) + 2^{-\Omega(\lambda)},$ 

where  $Adv_{MDDH}(\mathcal{A})$  and  $Adv_{CDH}(\mathcal{A})$  are the advantage function for the MDDH problem [13] and the CDH problem.

Acknowledgements. We would like to thank the reviewers for their valuable comments. This work was partially supported by Guangdong Major Project of Basic and Applied Basic Research (2019B030302008), National Natural Science Foundation of China under Grant 61925207 and Grant 62372292, and the National Key R&D Program of China under Grant 2022YFB2701500.

#### References

 Barbosa, M., Gellert, K., Hesse, J., Jarecki, S.: Bare PAKE: universally composable key exchange from just passwords. In: Reyzin, L., Stebila, D. (eds.) CRYPTO 2024, Part II. LNCS, vol. 14921, pp. 183–217. Springer (2024), https://doi.org/10. 1007/978-3-031-68379-4\_6

- Beguinet, H., Chevalier, C., Pointcheval, D., Ricosset, T., Rossi, M.: GeT a CAKE: Generic transformations from key encaspulation mechanisms to password authenticated key exchanges. In: Tibouchi, M., Wang, X. (eds.) ACNS 23, Part II. LNCS, vol. 13906, pp. 516–538. Springer, Heidelberg (Jun 2023). https://doi.org/10.1007/978-3-031-33491-7\_19
- Bellovin, S.M., Merritt, M.: Augmented encrypted key exchange: A password-based protocol secure against dictionary attacks and password file compromise. In: Denning, D.E., Pyle, R., Ganesan, R., Sandhu, R.S., Ashby, V. (eds.) ACM CCS 93. pp. 244–250. ACM Press (Nov 1993). https://doi.org/10.1145/168588.168618
- Benhamouda, F., Pointcheval, D.: Verifier-based password-authenticated key exchange: New models and constructions. Cryptology ePrint Archive, Report 2013/833 (2013), https://eprint.iacr.org/2013/833
- 5. Bernstein, D.J., Hülsing, A., Kölbl, S., Niederhagen, R., Rijneveld, J., Schwabe, P.: The SPHINCS<sup>+</sup> signature framework. In: Cavallaro, L., Kinder, J., Wang, X., Katz, J. (eds.) ACM CCS 2019. pp. 2129–2146. ACM Press (Nov 2019). https: //doi.org/10.1145/3319535.3363229
- Boneh, D., Dagdelen, Ö., Fischlin, M., Lehmann, A., Schaffner, C., Zhandry, M.: Random oracles in a quantum world. In: Lee, D.H., Wang, X. (eds.) ASI-ACRYPT 2011. LNCS, vol. 7073, pp. 41–69. Springer, Heidelberg (Dec 2011). https://doi.org/10.1007/978-3-642-25385-0\_3
- Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., Stehlé, D.: Crystals-kyber: a cca-secure module-latticebased kem. In: 2018 IEEE European Symposium on Security and Privacy (EuroS&P). pp. 353–367. IEEE (2018)
- Canetti, R.: Universally composable security: A new paradigm for cryptographic protocols. In: 42nd FOCS. pp. 136–145. IEEE Computer Society Press (Oct 2001). https://doi.org/10.1109/SFCS.2001.959888
- Canetti, R., Halevi, S., Katz, J., Lindell, Y., MacKenzie, P.D.: Universally composable password-based key exchange. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 404–421. Springer, Heidelberg (May 2005). https://doi. org/10.1007/11426639\_24
- D'Anvers, J.P., Karmakar, A., Roy, S.S., Vercauteren, F.: Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM. In: Joux, A., Nitaj, A., Rachidi, T. (eds.) AFRICACRYPT 18. LNCS, vol. 10831, pp. 282–305. Springer, Heidelberg (May 2018). https://doi.org/10.1007/ 978-3-319-89339-6\_16
- Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, D.: CRYSTALS-Dilithium: A lattice-based digital signature scheme. IACR TCHES 2018(1), 238-268 (2018). https://doi.org/10.13154/tches.v2018.i1.238-268, https://tches.iacr.org/index.php/TCHES/article/view/839
- Duman, J., Hartmann, D., Kiltz, E., Kunzweiler, S., Lehmann, J., Riepel, D.: Generic models for group actions. In: Boldyreva, A., Kolesnikov, V. (eds.) PKC 2023, Part I. LNCS, vol. 13940, pp. 406–435. Springer, Heidelberg (May 2023). https://doi.org/10.1007/978-3-031-31368-4\_15
- Escala, A., Herold, G., Kiltz, E., Ràfols, C., Villar, J.: An algebraic framework for Diffie-Hellman assumptions. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part II. LNCS, vol. 8043, pp. 129–147. Springer, Heidelberg (Aug 2013). https: //doi.org/10.1007/978-3-642-40084-1\_8
- Fouque, P.A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte, W., Zhang, Z., et al.: Falcon: Fast-fourier

lattice-based compact signatures over ntru. Submission to the NISTs post-quantum cryptography standardization process 36(5), 1–75 (2018)

- Gentry, C., MacKenzie, P., Ramzan, Z.: A method for making password-based key exchange resilient to server compromise. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 142–159. Springer, Heidelberg (Aug 2006). https://doi. org/10.1007/11818175\_9
- Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Ladner, R.E., Dwork, C. (eds.) 40th ACM STOC. pp. 197–206. ACM Press (May 2008). https://doi.org/10.1145/ 1374376.1374407
- Gu, Y., Jarecki, S., Krawczyk, H.: KHAPE: Asymmetric PAKE from key-hiding key exchange. In: Malkin, T., Peikert, C. (eds.) CRYPTO 2021, Part IV. LNCS, vol. 12828, pp. 701–730. Springer, Heidelberg, Virtual Event (Aug 2021). https: //doi.org/10.1007/978-3-030-84259-8\_24
- Hesse, J.: Separating symmetric and asymmetric password-authenticated key exchange. In: Galdi, C., Kolesnikov, V. (eds.) SCN 20. LNCS, vol. 12238, pp. 579–599. Springer, Heidelberg (Sep 2020). https://doi.org/10.1007/ 978-3-030-57990-6\_29
- Hwang, J.Y., Jarecki, S., Kwon, T., Lee, J., Shin, J.S., Xu, J.: Round-reduced modular construction of asymmetric password-authenticated key exchange. In: Catalano, D., De Prisco, R. (eds.) SCN 18. LNCS, vol. 11035, pp. 485–504. Springer, Heidelberg (Sep 2018). https://doi.org/10.1007/978-3-319-98113-0\_26
- Januzelli, J., Roy, L., Xu, J.: Under what conditions is encrypted key exchange actually secure? Cryptology ePrint Archive, Paper 2024/324 (2024), https:// eprint.iacr.org/2024/324
- Langlois, A., Stehlé, D.: Worst-case to average-case reductions for module lattices. DCC 75(3), 565–599 (2015). https://doi.org/10.1007/s10623-014-9938-4
- Liu, X., Liu, S., Han, S., Gu, D.: EKE meets tight security in the Universally Composable framework. In: Boldyreva, A., Kolesnikov, V. (eds.) PKC 2023, Part I. LNCS, vol. 13940, pp. 685–713. Springer, Heidelberg (May 2023). https://doi. org/10.1007/978-3-031-31368-4\_24
- Lyubashevsky, V.: Lattice signatures without trapdoors. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 738–755. Springer, Heidelberg (Apr 2012). https://doi.org/10.1007/978-3-642-29011-4\_43
- McQuoid, I., Xu, J.: An efficient strong asymmetric pake compiler instantiable from group actions. In: ASIACRYPT 2023. pp. 176-207. Springer (2023), https: //eprint.iacr.org/2023/1434
- Okamoto, T., Pointcheval, D.: REACT: Rapid Enhanced-security Asymmetric Cryptosystem Transform. In: Naccache, D. (ed.) CT-RSA 2001. LNCS, vol. 2020, pp. 159–175. Springer, Heidelberg (Apr 2001). https://doi.org/10.1007/3-540-45353-9\_13
- Pan, J., Wagner, B., Zeng, R.: Lattice-based authenticated key exchange with tight security. In: Handschuh, H., Lysyanskaya, A. (eds.) CRYPTO 2023, Part V. LNCS, vol. 14085, pp. 616–647. Springer, Heidelberg (Aug 2023). https://doi.org/10. 1007/978-3-031-38554-4\_20
- Pan, J., Zeng, R.: A generic construction of tightly secure password-based authenticated key exchange. In: Guo, J., Steinfeld, R. (eds.) ASIACRYPT 2023, Part VIII. LNCS, vol. 14445, pp. 143–175. Springer, Heidelberg (Dec 2023). https://doi.org/10.1007/978-981-99-8742-9\_5

- Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Gabow, H.N., Fagin, R. (eds.) 37th ACM STOC. pp. 84–93. ACM Press (May 2005). https://doi.org/10.1145/1060590.1060603
- 29. Santos, B.F.D., Gu, Y., Jarecki, S.: Randomized half-ideal cipher on groups with applications to UC (a)PAKE. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023, Part V. LNCS, vol. 14008, pp. 128–156. Springer, Heidelberg (Apr 2023). https://doi.org/10.1007/978-3-031-30589-4\_5
- Santos, B.F.D., Gu, Y., Jarecki, S., Krawczyk, H.: Asymmetric PAKE with low computation and communication. In: Dunkelman, O., Dziembowski, S. (eds.) EU-ROCRYPT 2022, Part II. LNCS, vol. 13276, pp. 127–156. Springer, Heidelberg (May / Jun 2022). https://doi.org/10.1007/978-3-031-07085-3\_5
- 31. Schmidt, J.: Requirements for password-authenticated key agreement (pake) schemes. Tech. rep. (2017), https://tools.ietf.org/html/rfc8125
- 32. Shoup, V.: Security analysis of itSPAKE2+. In: Pass, R., Pietrzak, K. (eds.) TCC 2020, Part III. LNCS, vol. 12552, pp. 31–60. Springer, Heidelberg (Nov 2020). https://doi.org/10.1007/978-3-030-64381-2\_2

# Appendix

# A Full Descriptions of Simulator Sim

The simulator  $\mathsf{Sim}$  in  $\mathsf{G}_7$  is presented in Fig. 6 and Fig. 7.

nitialization
im maintains lists $\mathcal{L}_{H_0}, \mathcal{L}_{H_1}, \mathcal{L}_{H_2}, \mathcal{L}_{H_3}, \mathcal{L}_{H_4}$ , sent, recv (all initialized to be empty) in the simulation
• $\mathcal{L}_{H_0}, \mathcal{L}_{H_1}, \mathcal{L}_{H_2}, \mathcal{L}_{H_3}, \mathcal{L}_{H_4}$ : store records to simulate random oracles $H_0, H_1, H_2, H_3$ and $H_4$
• sent : store messages sent by client/server instances
• recv : store messages received by client/server instances
im outputs $crs := (H_0, H_1, H_2, H_3, H_4)$
tealing Password Data
n (StealPWFile, $C^{(i)}$ , $S^{(j)}$ ) from $\mathcal{F}_{apake}$ :
If $\mathcal{F}_{apake}$ additionally returns $pw$ , set $rw := H_0(pw)$ and $r := H_1(pw)$ , record $(C^{(i)}, S^{(j)}, pw, rw, r)$ .
Otherwise, set $rw \leftarrow \{0,1\}^{\lambda}$ , $r \leftarrow \mathcal{R}$ , record $(C^{(i)},S^{(j)},?,rw,r)$ .
Generate $(pk, sk) \leftarrow KeyGen(r)$ , and mark the record $(C^{(i)}, S^{(j)}, \cdot, rw, r)$ as <b>stolen</b> , return $(rw, pk)$ to $\mathcal{A}$ .
deal PAKE Sessions
n (NewClient, $C^{(i)}$ , <i>iid</i> , $S^{(j)}$ ) from $\mathcal{F}_{apake}$ :
Record $(C^{(i)}, iid, S^{(j)}, ?)$ and mark it as <b>fresh</b> , send (NewClient, $C^{(i)}, iid, S^{(j)}$ ) from $\mathcal{F}_{pake}$ to $\mathcal{A}$ .
n (NewServer, $S^{(j)},  iid',  C^{(i)})$ from $\mathcal{F}_{apake}$ :
Record $(S^{(j)}, iid', C^{(i)}, ?)$ and mark it as <b>fresh</b> , send (NewServer, $S^{(j)}, iid', C^{(i)}$ ) from $\mathcal{F}_{pake}$ to $\mathcal{A}$ .
n (Testpw, $P, iid, rw'$ ) from $A$ :
If there exists $(pw', rw') \in \mathcal{L}_{H_0}$ , send (Testpw, $P, iid, pw'$ ) to $\mathcal{F}_{apake}$ , and forward $\mathcal{F}_{apake}$ 's answer to $\mathcal{A}$ .
If $\mathcal{F}_{apake}$ returns "correct guess", frecord $(C^{(i)},S^{(j)},pw',H_0(pw'),H_1(pw'))$ .
If there exists a record (NewClient/NewServer, $P, iid, Q$ ) and a stolen record $(P, Q, \cdot, rw, r)$ or $(Q, P, \cdot, rw, r)$ with
$rw = rw'$ , then return "correct guess" to $\mathcal{A}$ .
In any other cases, return "wrong guess" to $\mathcal{A}$ .
If Sim returns "correct guess", mark record $(P, iid, Q, (H_0(pw)/rw, H_1(pw)/r))$ as compromised.
Otherwise, mark record $(P, iid, Q, ?)$ as interrupted.
n (NewKey, $P$ , $iid$ , $sid$ , $Key^*$ ) from $A$ :
If there is a <b>compromised</b> record $(P, iid, Q, (rw, r))$ , send $(sid, Key := Key^*)$ to $P$ .
If there exists a <b>fresh</b> record $(P, iid, Q, \cdot)$ and a completed record $(Q, iid', P, \cdot)$ , $(sid, Key')$ was sent
to Q and $(Q, iid', P, \cdot)$ was <b>fresh</b> at the time, then return $(sid, Key := Key')$ to P.
In any other cases, pick a random key Key $\leftarrow$ s $\{0,1\}^{\lambda}$ , send $(sid, Key)$ to P.
Finally, mark the record $(P, iid, Q, \cdot)$ as <b>completed</b> and record $(P, iid, sid, Key)$ .

Fig. 6: Simulator Sim part I.

```
Additional aPAKE operations
Generating \psi for server instance (S^{(j)}, iid'):
   Retrieve record (S^{(j)}, iid', sid, Key).
   If there exists a compromised record (S^{(j)}, iid', C^{(i)}, (rw, r)), then compute (pk, sk) \leftarrow \mathsf{KeyGen}(r),
   (c, K_1) \leftarrow \mathsf{Encap}(pk), and \psi \leftarrow \mathsf{AE}.\mathsf{Enc}(H_2(\mathsf{Key}), c). Otherwise, compute \psi \leftarrow \mathsf{AE}.\mathsf{Enc}(H_2(\mathsf{Key}), 0) and set K_1 := \bot.
   Return \psi from S^{(j)} to \mathcal{A}, sent := sent \cup \{S^{(j)}, iid', sid, \psi, K_1\}.
on \psi from \mathcal{A} as a server message from \mathsf{S}^{(j)} to (\mathsf{C}^{(i)}, iid):
   \mathsf{recv} := \mathsf{recv} \cup \{\mathsf{C}^{(i)}, iid, sid, \psi\}
   Retrieve record (C^{(i)}, iid, sid, Key).
   If there are no compromised records (C^{(i)}, iid, S^{(j)}, (rw, r)):
      If there exists record (S^{(j)}, iid', sid, \psi, K_1) \in sent:
          Generate \sigma \leftarrow \{0,1\}^{\lambda}, send (FreshKey, C^{(i)}, iid, sid |\psi|\sigma) to \mathcal{F}_{apake}, and return \sigma from C^{(i)} to \mathcal{A}.
      If there are no records (S^{(j)}, iid', sid, \psi) \in sent:
          Reject the session by sending (Abort, C^{(i)}, iid) to \mathcal{F}_{apake}.
   Else there exists compromised records (C^{(i)}, iid, S^{(j)}, (rw, r)):
      Compute c \leftarrow \mathsf{AE}.\mathsf{Dec}(H_2(\mathsf{Key}), \psi).
      If c = \bot: reject the session by sending (Abort, C^{(i)}, iid) to \mathcal{F}_{apake}.
      Else:
          If there exists a stolen record (C^{(i)}, S^{(j)}, \cdot, rw, r), send (Impersonate, C^{(i)}, iid) to \mathcal{F}_{apake}.
          Generate (pk, sk) \leftarrow \mathsf{KeyGen}(r), decrypt K_1 \leftarrow \mathsf{Decap}(sk, c), compute \sigma := H_3(\mathsf{Key}, K_1, sid|\psi),
         send (CorruptKey, C^{(i)}, iid, sid |\psi|\sigma, H_4(Key)) to \mathcal{F}_{apake}, return \sigma from C^{(i)} to \mathcal{A}.
on \sigma from \mathcal{A} as a client message from C^{(i)} to (S^{(j)}, iid'):
   Retrieve record (S^{(j)}, iid', sid, Key).
   If \exists (S^{(j)}, iid', sid, \psi, K_1) \in \text{sent} \land (C^{(i)}, iid, sid, \psi) \in \text{recv} \land (C^{(i)}, iid, sid, \sigma) \in \text{sent}:
          Send (FreshKey, S^{(j)}, iid', sid|\psi|\sigma) to \mathcal{F}_{apake}.
   Retrieve K_1 from record (S^{(j)}, iid', sid, \psi, K_1)
   If Sim queried (Testpw, S^{(j)}, iid', pw) to \mathcal{F}_{apake} before and obtained "correct guess":
      If \sigma = H_3(\text{Key}, K_1, sid|\psi): send (CorruptKey, S^{(j)}, iid', sid|\psi|\sigma, H_4(\text{Key})) to \mathcal{F}_{apake}.
   If Sim queried (OfflineTestPW, C^{(i)}, S^{(j)}, pw) before and obtained "correct guess":
      If \sigma = H_3(\text{Key}, K_1, sid|\psi): send (CorruptKey, S^{(j)}, iid', sid|\psi|\sigma, H_4(\text{Key})) to \mathcal{F}_{apake}.
   In any other cases: send (Abort, S^{(j)}, iid') to \mathcal{F}_{apake}.
Random Oracles
on H_0(pw, \mathsf{C}^{(i)}, \mathsf{S}^{(j)}) from \mathcal{A}:
   If \exists (pw, \mathsf{C}^{(i)}, \mathsf{S}^{(j)}, Y) \in \mathcal{L}_{H_0}: return Y
   Else send (OfflineTestPW, C^{(i)}, S^{(j)}, pw) to \mathcal{F}_{apake} and if it returns "correct guess":
      Update the stolen record with (\mathsf{C}^{(i)},\mathsf{S}^{(j)},pw,rw,r), \mathcal{L}_{H_0} := \mathcal{L}_{H_0} \cup \{(pw,rw)\}, \mathcal{L}_{H_1} := \mathcal{L}_{H_1} \cup \{(pw,r)\}, return rw.
   In any other cases: Y \leftarrow \{0,1\}^{\lambda}, \mathcal{L}_{H_0} := \mathcal{L}_{H_0} \cup \{(pw, \mathsf{C}^{(i)}, \mathsf{S}^{(j)}, Y)\}, and return Y.
on H_1(pw, \mathsf{C}^{(i)}, \mathsf{S}^{(j)}) from \mathcal{A}:
  If \exists (pw, \mathsf{C}^{(i)}, \mathsf{S}^{(j)}, Y) \in \mathcal{L}_{H_1}: return Y
   Else send (OfflineTestPW, C^{(i)}, S^{(j)}, pw) to \mathcal{F}_{apake} and if it returns "correct guess":
      Update the stolen record with (\mathsf{C}^{(i)},\mathsf{S}^{(j)}, pw, rw, r), \mathcal{L}_{H_0} := \mathcal{L}_{H_0} \cup \{(pw, rw)\}, \mathcal{L}_{H_1} := \mathcal{L}_{H_1} \cup \{(pw, r)\}, \text{return } r.
   In any other cases: Y \leftarrow R, \mathcal{L}_{H_1} := \mathcal{L}_{H_1} \cup \{(pw, \mathsf{C}^{(i)}, \mathsf{S}^{(j)}, Y)\}, and return Y.
on H_i(X) from \mathcal{A} for i \in \{2, 3, 4\}:
   If \exists (X, Y) \in \mathcal{L}_{H_i}: return Y
   Else: Y \leftarrow \{0,1\}^{\lambda}, \mathcal{L}_{H_i} := \mathcal{L}_{H_i} \cup \{(X,Y)\}, and return Y.
```

Fig. 7: Simulator Sim part II.

### B Proof of Theorem 2: Tight Reduction for Our aPAKE Compiler from OW-ChCCA Secure KEM

If the underlying KEM in our compiler has OW-ChCCA security, then our our compiler becomes a tightness-preserving one, as shown in Theorem 2. In this section, we will present the proof for Theorem 2.

We first recall the OW-ChCCA security [26] for KEM.

**Definition 6 (OW-ChCCA security for KEM** [26]). For a KEM scheme KEM = (KeyGen, Encap, Decap), the advantage function of an adversary  $\mathcal{A}$  for N users and  $\ell$  challenges is defined by  $\mathsf{Adv}_{\mathsf{KEM}}^{(N,\ell)-\mathsf{ChCCA}}(\mathcal{A}) := \Pr\left[\mathsf{OW-ChCCA}_{\mathsf{KEM}}^{\mathcal{A}} \Rightarrow 1\right]$ , where experiment OW-ChCCA $_{\mathsf{KEM}}^{\mathcal{A}}$  is defined in Fig. 8. The OW-ChCCA security for KEM requires  $\mathsf{Adv}_{\mathsf{KEM}}^{(N,\ell)-\mathsf{ChCCA}}(\mathcal{A}) = \mathsf{negl}(\lambda)$  for all PPT  $\mathcal{A}$ .

$OW\operatorname{-ChCCA}_{KFM}^{\mathcal{A}}(\lambda):$	<b>Oracle</b> $CORR(i)$
$\frac{p \leftarrow Setup(1^{\lambda})}{pp} \leftarrow Setup(1^{\lambda})$	$\mathcal{L}_{\text{CORR}} := \mathcal{L}_{\text{CORR}} \cup \{i\}$
For $i \in [N]$ :	return $r_i$
$\begin{array}{c} r_i \leftarrow R \end{array}$	·
$(pk_i, sk_i = r_i) \leftarrow \text{Gen}(pp; r_i)$	<b>Oracle</b> $Dec(i, c')$
$O := \{ ENC, DEC, REVEAL, CORR, CHECK \}$	If $\exists K' \text{ s.t. } (i, c', K') \in \mathcal{L}_{\text{ENC}}$ : return $\perp$
$(i^*, c^*, K^*) \leftarrow \mathcal{A}^O(pp, (pk_i)_{i \in [N]})$	return $K' := Decap(sk_i, c')$
If $(i^*, c^*, K^*) \notin \mathcal{L}_{ENC}$ : return 0	
If $i^* \in \mathcal{L}_{\text{CORR}}$ : return 0	<b>Oracle</b> $ENC(i)$ :
If $(i^*, c^*) \in \mathcal{L}_{\text{REVEAL}}$ : return 0	If $ \mathcal{L}_{\text{ENC}}  \geq \ell$ : return $\perp$
If $CHECK(i^*, c^*, K^*) = 1$ : return 1	$(c, K) \leftarrow Encap(pk_i)$
	$\mathcal{L}_{\mathrm{ENC}} := \mathcal{L}_{\mathrm{ENC}} \cup \{(i, c, K)\}$
<b>Oracle</b> REVEAL $(i, c)$ :	return c
<b>If</b> $\exists K$ s.t. $(i, c, K) \in \mathcal{L}_{ENC}$ :	
$\mathcal{L}_{\text{REVEAL}} := \mathcal{L}_{\text{REVEAL}} \cup \{(i, c)\}$	<b>Oracle</b> $CHECK(i, c, K)$
return K	If $Decap(sk_i, c) = K$ :
$\mathbf{return} \perp$	return 1
	return 0

Fig. 8: The OW-ChCCA security experiment for KEM.

Note that we take KEM as a canonical one, where the randomness  $r_i$  used in Gen is taken as the secret key  $sk_i$ . That is reflected in the OW-ChCCA security experiment, where the CORR oracle outputs the randomness  $r_i$  which is used to derive the key pair  $(pk_i, sk_i)$ .

In [26], Pan et. al proposed a specific tightly OW-ChCCA secure KEM based on the Matrix DDH assumption in the RO model. We review their KEM in Fig.10.

Next we recall Theorem 2 and present its proof.

**Theorem 2.** If KEM is a KEM with OW-ChCCA security, AE is the informationtheoretically secure AE (shown in Sect. 4) with one-time authenticity and onetime CCA security,  $H_0, H_1, H_2, H_3, H_4$  work as random oracles, then the aPAKE scheme in Fig. 5 securely emulates  $\mathcal{F}_{apake}$ , hence achieving UC security in the  $\{\mathcal{F}_{pake}, \mathcal{F}_{RO}\}$ -hybrid model. More precisely, suppose there are at most N parties and  $\ell$  sessions, and  $\mathcal{A}$  issues q random oracle queries, then there exists a simulator Sim such that

$$\left|\Pr\left[\mathbf{Real}_{\mathcal{Z},\mathcal{A}}\right] - \Pr\left[\mathbf{Ideal}_{\mathcal{Z},\mathsf{Sim}}\right]\right| \le \mathsf{Adv}_{\mathsf{KEM}}^{(N^2,\ell)-\mathsf{ChCCA}}(\mathcal{B}_{\mathsf{KEM}}) + \frac{2\ell + q^2 + q + 1}{2^{\lambda}}.$$
(1)

*Proof.* Recall that if we use the information-theoretically secure AE scheme  $AE_{it}$  in our compiler, then  $Adv_{AE}^{ot-auth}(\mathcal{B}_{AE}) = Adv_{AE}^{ot-cca}(\mathcal{B}_{AE}) = 1/2^{\lambda}$ . Consequently, the security loss in the proof of Theorem 1 owes to the reduction between  $G_7$  and  $G_6$ , which is based on the OW-PCA security of KEM. Now we show that if KEM has OW-ChCCA security, then the reduction between  $G_7$  and  $G_6$  can be a tight one, and our compiler becomes a tightness-preserving one captured by (1).

Below we will give a tight reduction between  $G_7$  and  $G_6$  based on the OW-ChCCA security of KEM.

Recall that  $G_7$  and  $G_6$  differ only when event **Bad** happens.

**Bad:** Case II occurs to some  $(S^{(j)}, iid')$ ,  $\sigma = H_3(K_0, K_1, sid|\psi)$ , but until then none of the Sim's (OfflineTestPW,  $C^{(i)}, S^{(j)}, pw'$ ) queries results in "correct guess".

With difference lemma, we know that  $|\Pr[\mathsf{G}_7 \Rightarrow 1] - \Pr[\mathsf{G}_6 \Rightarrow 1]| \leq \Pr[\mathbf{Bad} \text{ in } \mathsf{G}_7]$ . Next we show a reduction algorithm  $\mathcal{B}_{\mathsf{KEM}}$  and prove  $\Pr[\mathbf{Bad} \text{ in } \mathsf{G}_7] \leq \mathsf{Adv}_{\mathsf{KEM}}^{(N^2,\ell)-\mathsf{ChCCA}}$ .

 $\mathcal{B}_{\mathsf{KEM}}$  obtains at most  $N^2$  public keys  $pk_{\mathsf{C}^{(i)}}^{\mathsf{S}^{(j)}}$  for each pair of  $(\mathsf{C}^{(i)},\mathsf{S}^{(j)})$  and has access to oracles defined in Fig. 8.

In the reduction,  $\mathcal{B}_{KEM}$  plays the role of the simulator Sim in  $G_7$ .  $\mathcal{B}_{KEM}$  does the simulations as follows.

- Before receiving (StealPWFile,  $C^{(i)}, S^{(j)}$ ) from  $\mathcal{A}$ :  $\mathcal{B}_{KEM}$  behaves just like Sim does in  $G_7$ .
- Upon receiving (StealPWFile,  $C^{(i)}, S^{(j)}$ ) from  $\mathcal{A}: \mathcal{B}_{\mathsf{KEM}}$  issues a StealPWFile query to  $\mathcal{F}_{apake}$ . If  $\mathcal{F}_{apake}$  replies with pw and "correct guess", then  $\mathcal{B}_{\mathsf{KEM}}$ behaves just like Sim does in  $\mathsf{G}_7$ . More precisely,  $\mathcal{B}_{\mathsf{KEM}}$  computes rw := $H_0(pw)$ , sets the trapdoor record as  $(C^{(i)}, S^{(j)}, rw, pk, sk, H_1(pw))$  where  $(pk, sk) \leftarrow \mathsf{KeyGen}(H_1(pw))$ , and returns the password file (rw, pk). Otherwise,  $\mathcal{B}_{\mathsf{KEM}}$  randomly samples  $rw \leftarrow \{0,1\}^{\lambda}$ , sets the trapdoor record as  $(C^{(i)}, \mathsf{S}^{(j)}, rw, pk_{\mathsf{C}^{(i)}}^{\mathsf{S}^{(j)}}, sk =?, r=?)$ , and returns the password file  $(rw, pk_{\mathsf{C}^{(i)}}^{\mathsf{S}^{(j)}})$ to  $\mathcal{A}$ .
- After receiving (StealPWFile,  $C^{(i)}, S^{(j)}$ ) from  $\mathcal{A}$ : During this phase, for any offline attack from  $\mathcal{A}$ , if the corresponding (OfflineTestPW,  $C^{(i)}, S^{(j)}, pw'$ ) query to  $\mathcal{F}_{apake}$  results in "correct guess", then **Bad** does not happen on any

session between instances  $(C^{(i)}, iid)$  and  $(S^{(j)}, iid')$ . In this case,  $\mathcal{B}_{\mathsf{KEM}}$  queries  $\operatorname{CORR}(C^{(i)}, S^{(j)})$  from its OW-ChCCA challenger to obtain the randomness r and then re-programmes  $H_0(pw, C^{(i)}, S^{(j)}) := rw$  and  $H_1(pw, C^{(i)}, S^{(j)}) := r$ . Then  $\mathcal{B}_{\mathsf{KEM}}$  updates its trapdoor record to  $(C^{(i)}, S^{(j)}, rw, pk_{C^{(i)}}^{S^{(j)}}, sk_{C^{(i)}}^{S^{(j)}}, r)$ .

For the session between instances  $(C^{(i)}, iid)$  and  $(S^{(j)}, iid')$ ,  $\mathcal{B}_{\mathsf{KEM}}$  first simulates the generation of PAKE key  $K_0$  without pw and trapdoor record, just like Sim. If Case II does not happen to instance  $(C^{(i)}, iid)$  or  $(S^{(j)}, iid')$ , then **Bad** event cannot happen to  $(S^{(j)}, iid')$  and  $\mathcal{B}_{\mathsf{KEM}}$  can simulate them without neither password pw nor the trapdoor record just like Sim does in  $G_7$ . We show how  $\mathcal{B}_{\mathsf{KEM}}$  simulates instances  $(C^{(i)}, iid)$  and  $(S^{(j)}, iid')$  in Case II below.

For server instance  $(S^{(j)}, iid')$ ,  $\mathcal{B}_{\mathsf{KEM}}$  can simulate the generation of  $\psi$ . If  $\mathcal{F}_{apake}$  returned pw and "correct guess" before, then  $\mathcal{B}_{\mathsf{KEM}}$  generates  $\psi$  just like Sim does in  $G_7$ . Otherwise,  $\mathcal{B}_{\mathsf{KEM}}$  queries its challenge oracle to obtain  $c^* \leftarrow \mathsf{Enc}(\mathsf{C}^{(i)},\mathsf{S}^{(j)})$  to obtain a challenge ciphertext  $c^*$ . Then  $\mathcal{B}_{\mathsf{KEM}}$  invokes  $\psi \leftarrow \mathsf{AE}.\mathsf{Enc}(\mathcal{H}_2(K_0), c^*)$ . Since  $c^*$  is an encapsulation under  $pk_{\mathsf{C}^{(i)}}^{\mathsf{S}^{(j)}}$ ,  $\mathcal{B}_{\mathsf{KEM}}$ 's simulation of  $\psi$  is perfect.

For client instance  $(C^{(i)}, iid)$ , if  $\mathcal{B}_{\mathsf{KEM}}$  has the trapdoor record  $(C^{(i)}, S^{(j)}, rw, pk, sk \neq ?, r)$ , then  $\mathcal{B}_{\mathsf{KEM}}$  can use sk to simulate  $\sigma$  and the session key just like Sim does in  $G_7$ . Otherwise,  $\mathcal{B}_{\mathsf{KEM}}$  has no  $sk = sk_{\mathsf{C}^{(i)}}^{S(j)}$  now. To simulate  $\sigma$  and the session key,  $\mathcal{B}_{\mathsf{KEM}}$  resorts to ROs and the re-programming techniques: upon  $(C^{(i)}, iid)$  receiving  $\psi'$ ,  $\mathcal{B}_{\mathsf{KEM}}$  invokes  $c \leftarrow \mathsf{AE}.\mathsf{Dec}(H_2(K_0),\psi')$ . If  $c = \bot$ ,  $\mathcal{B}_{\mathsf{KEM}}$  behaves just like Sim (no  $sk_{\mathsf{C}^{(i)}}^{S(j)}$  involved). If  $c \neq \bot$ , for all hash queries  $H_3(K_0, K_1, sid|\psi')$ ,  $\mathcal{B}_{\mathsf{KEM}}$  first checks whether there exists  $K_1$  such that  $\mathsf{CHECK}(\mathsf{C}^{(i)},\mathsf{S}^{(j)}, c, K_1) = 1$ , if yes, set  $\sigma := H_3(K_0, K_1, sid|\psi')$ . Otherwise, randomly choose  $\sigma \leftarrow s \{0, 1\}^{\lambda}$ , and set  $H_3(K_0, ?, sid|\psi') := \sigma$  with ? denoting the undermined value of  $K_1$ . It then returns  $\sigma$  to  $\mathcal{A}$  and returns  $\mathsf{sKey} := H_2(K_0)$  as the session key. If later  $\mathcal{A}$  issues any new query  $H_3(K_0, K'_1, sid|\psi')$ ,  $\mathcal{B}_{\mathsf{KEM}}$  checks whether  $\mathsf{CHECK}(c, K'_1) = 1$ . If yes,  $\mathcal{B}_{\mathsf{KEM}}$  re-programme  $H_3(K_0, K'_1, sid|\psi') := \sigma$ .

Upon  $(S^{(j)}, iid')$  receiving  $\sigma'$ . If there is no  $H_3$  query such that  $\sigma' = H_3(K_0, K'_1, sid|\psi)$ , then  $\sigma' = H_3(K_0, K_1, sid|\psi)$  with negligible probability.  $\mathcal{B}_{\mathsf{KEM}}$  sends  $(\mathsf{Abort}, \mathsf{S}^{(j)}, iid')$ to  $\mathcal{F}_{apake}$ , and accordingly  $\mathcal{F}_{apake}$  returns  $\bot$ , sKey :=  $\bot$  to  $(\mathsf{S}^{(j)}, iid')$  to reject the session. Otherwise, from  $\mathcal{A}$  hash query such that  $\sigma' = H_3(K_0, K'_1, sid|\psi)$ ,  $\mathcal{B}_{\mathsf{KEM}}$  checks whether  $\mathsf{CHECK}(\mathsf{C}^{(i)}, \mathsf{S}^{(j)}, c, K'_1) = 1$ . If no, then  $\sigma' \neq H_3(K_0, K_1 =$  $\mathsf{Decap}(sk_{\mathsf{C}^{(i)}}^{\mathsf{S}^{(j)}}, c^*), sid|\psi)$  and  $\mathcal{B}_{\mathsf{KEM}}$  sends  $(\mathsf{Abort}, \mathsf{S}^{(j)}, iid')$  to  $\mathcal{F}_{apake}$ . If yes,  $\mathsf{CHECK}(\mathsf{C}^{(i)}, \mathsf{S}^{(j)}, c^*, K'_1) =$ 1 implies  $K'_1 = \mathsf{Decap}(sk_{\mathsf{C}^{(i)}}^{\mathsf{S}^{(j)}}, c^*)$ . Then  $\mathcal{B}_{\mathsf{KEM}}$  sends  $(\mathsf{CorruptKey}, \mathsf{S}^{(j)}, iid', sid|\psi|\sigma', H_4(K_0))$ to  $\mathcal{F}_{apake}$ . Then  $\mathcal{F}_{apake}$  returns  $H_4(K_0)$  to  $(\mathsf{S}^{(j)}, iid')$ .

Note that during the whole simulation,  $\mathcal{B}_{\mathsf{KEM}}$  never queries DEC oracle and REVEAL oracle.  $\mathcal{B}_{\mathsf{KEM}}$  only queries CORR oracle if  $\mathcal{F}_{apake}$  returns pw and "correct guess" corresponding to some OfflineTestPW query. Therefore, if Bad event happens,  $\mathcal{B}_{\mathsf{KEM}}$  does not query CORR oracle or REVEAL oracle corresponding to the challenge ciphertext  $c^*$  but successfully obtains the encapsulated key  $K_1 = \mathsf{Decap}(sk_{\mathsf{C}^{(i)}}^{\mathsf{S}^{(j)}}, c^*)$ . Finally,  $\mathcal{B}_{\mathsf{KEM}}$  submits  $(\mathsf{C}^{(i)}, \mathsf{S}^{(j)}, K_1)$  and wins the OW- ChCCA game. So we have

$$\left|\Pr\left[\mathsf{G}_{7} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_{6} \Rightarrow 1\right]\right| \leq \Pr\left[\mathsf{Bad} \text{ in } \mathsf{G}_{7}\right] \leq \mathsf{Adv}_{\mathsf{KEM}}^{(N^{2},\ell)\text{-}\mathsf{ChCCA}}$$

Collecting the statistical loss  $\frac{2\ell+q^2+q+1}{2^{\lambda}}$ , we obtain (1).

# C Proof of Lemma 1: Security Proof for the Information-Theoretic AE Scheme

Recall that our AE construction works as follows.

- $AE.Enc(k = (k_1, k_2, k_3), m)$ : it generates a ciphertext  $c = (c_1 = k_1 + m, c_2 = k_2 \times c_1 + k_3)$ .
- $AE.Dec(k = (k_1, k_2, k_3), c = (c_1, c_2))$ : it first checks whether  $c_2 = k_2 \times c_1 + k_3$ . If yes, it outputs  $c_1 - k_1$ . Otherwise, it outputs  $\perp$ .

Next we present the proof of the one-time authenticity and one-time CCA security of our AE.

<u>Proof of one-time authenticity</u>. The one-time authenticity considers an adversary  $\mathcal{A}$  who obtains an honestly generated challenge ciphertext of message  $m^*$  chosen by  $\mathcal{A}$ , i.e.,

$$c^* = (c_1^* = k_1 + m^*, c_2^* = c_1^* \times k_2 + k_3),$$

and requires that  $\mathcal{A}$  can hardly generate a new and valid ciphertext  $c = (c_1, c_2)$ such that  $c \neq c^*$  but  $\mathsf{AE.Dec}(k, c) \neq \bot$ , i.e.,  $c_2 = c_1 \times k_2 + k_3$ .

We consider the following two cases.

- **Case 1:**  $c_1 \neq c_1^*$ . In this case,  $c_2 = c_1 \times k_2 + k_3$  implies that  $k_2 = (c_2 c_2^*)/(c_1 c_1^*)$ . Due to the uniformity of key  $k_3$ ,  $c^* = (c_1^*, c_2^*)$  leaks no information of  $k_2$ . With the uniformity of key  $k_2$ , the event  $k_2 = (c_2 c_2^*)/(c_1 c_1^*)$  happens only with  $\frac{1}{2^{\lambda}}$ .
- **Case 2:**  $c_1 = \hat{c}_1^*$  **but**  $c_2 \neq c_2^*$ . In this case, the ciphertext c submitted by  $\mathcal{A}$  must be invalid since  $c_2 = c_1 \times k_2 + k_3 = c_1^* \times k_2 + k_3 = c_2^* \neq c_2$ .

Overall,  $\mathcal{A}$  can hardly generate a new valid ciphertext, except with probability at most  $1/2^{\lambda}$ , and the one-time authenticity follows.

<u>Proof of one-time CCA security.</u> The one-time CCA security asks  $\mathcal{A}$  to determine whether a challenge ciphertext  $c^* = (c_1^* = k_1 + m_b, c_2^* = k_2 \times c_1^* + k_3)$  encrypts  $m_0$  or  $m_1$ , where  $m_0$  and  $m_1$  are chosen by  $\mathcal{A}$  itself, even if  $\mathcal{A}$  has one-time access to the **Dec** oracle, which decrypts ciphertexts different from  $c^*$ .

Due to the one-time authenticity of AE (as we shown above), the adversary can hardly generate a new valid ciphertext, so the Dec oracle would always return  $\perp$  (except with probability at most  $1/2^{\lambda}$ ).

As such, only the challenge ciphertext  $c^* = (c_1^* = k_1 + m_b, c_2^* = c_1^* \times k_2 + k_3)$ might be useful for  $\mathcal{A}$  to learn the challenge bit b. However, by the uniformity of  $k_1, c_1^* = k_1 + m_b$  perfectly hides  $m_b$ . Consequently,  $m_b$  is hidden in  $c^*$  so that  $\mathcal{A}$  can hardly guess b correctly, except with advantage at most  $1/2^{\lambda}$ , and the one-time CCA security follows.

# D Comparison with Other aPAKE Compilers from Post-quantum Assumptions

Table 3: Efficiency comparison with aPAKE compilers [15] and [24]. For computing and communication cost, we use the mode of "Client + Server = Total" to reflect the separation of client/server computation/communication. Efficiency comparison with post-quantum aPAKE compilers in [15] instantiated from NIST PQC winner signature schemes and in [24] instantiated from CSIDH. All algorithms except Falcon are used in their versions of NIST security level 3 (i.e., security comparable to breaking AES-192). As for Falcon, we use its level 1 version, due to its lack of level 3.

aPAKE	Registration	Computing	Server	Communication	Assumption
Compiler	Time (ms)	Time (ms)	Storage (KB)	Cost (KB)	Туре
[15] (Dilithium)	0.096	0.245 + 0.126 = 0.371	5.875	3.215 + 3.938 = 7.153	Lattice-based
[15] (Falcon)	7.003	0.271 + 0.074 = 0.345	2.189	0.642 + 1.282 = 1.924	Lattice-based
[15] (Sphincs <sup>+</sup> -s)	23.505	230 + 0.4 = 230.4	0.203	15.86 + 0.12 = 15.98	Hash-based
[15] (Sphincs <sup>+</sup> -f)	0.385	10.4 + 0.8 = 11.2	0.203	34.83 + 0.12 = 34.95	Hash-based
[24] (CSIDH)	2514.011	3008 + 971 = 3979	0.25	0 + 0.125 = 0.125	Isogeny-based
Ours (Kyber)	0.017	0.051 + 0.083 = 0.134	1.188	0.031 + 1.094 = 1.125	Lattice-based

In Table 3, we compare our compiler with known aPAKE compilers instantiated from other post-quantum assumptions, including the signature-based compiler [15] and the isogeny-based compiler [24]. When [15] is instantiated with the NIST PQC hash-based signature scheme Sphincs<sup>+</sup>, they have smaller storage than ours, but their communication cost is dozens of times larger than ours and their registration time and computing time are dozens of times slower than ours. When the isogeny-based compiler [24] is instantiated with CSIDH, their server storage and communication cost are smaller than ours, but their registration time and computing time are ten thousands times slower than ours. This shows that our compiler overwhelms these compilers in terms of registration time and computing time, and has comparable server storage and communication cost.

### E Concrete aPAKE Schemes

#### E.1 Kyber-Based aPAKE Scheme from Lattices

By applying our Kyber-based compiler to the UC-secure Kyber-based PAKE scheme [2], we obtain A Kyber-based aPAKE scheme, which is shown in Fig. 9.

#### E.2 Tightly UC-Secure aPAKE Scheme from MDDH

By applying our MDDH-based compiler to the UC-secure CDH-based PAKE scheme [22], we obtain a tightly UC secure aPAKE scheme based on the MDDH assumption, which is shown in Fig. 11.

• Kyber = (Kyber.KeyGen, Ky		ст				
• Ideal ciphers $IC_1$ on domain $\mathcal{PK}$ and $IC_2$ on domain $\mathcal{CT}$ , where $\mathcal{PK}$ and $\mathcal{CT}$ are public key space and ciphertext space of Kyber.						
• Hash functions $H_0, H_2, H_3, G: \{0, 1\}^* \to \{0, 1\}^{\lambda}$ ,						
$H_1: \{0,1\}^* \to \mathcal{R}$	$//\mathcal{R}$ is the randomness s	pace of Kyber.KeyGen				
	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	F				
<u>Client <math>C^{(i)}</math></u> :		<u>Server <math>S^{(j)}</math></u> :				
	Registration -					
on input $pw$ :						
$rw := H_0(pw, C^{(i)}, S^{(j)});$						
$r := H_1(pw, C^{(i)}, S^{(j)})$	$\xrightarrow{rw, pk}$					
$(pk, sk) \leftarrow Kyber.KeyGen(r)$		store $(rw, pk)$				
	Login					
on input $pw$ :		on input $(rw, pk)$ :				
$(pk, sk) \leftarrow Kyber.KeyGen$						
$C_1 := IC_1.Enc(H_0(pw), \hat{pk})$						
	$C_1$	$\hat{pk} := IC_1.Dec(rw, C_1)$				
$\hat{c} := IC_2.Dec(H_0(pw), C_2)$		$(\hat{c}, \hat{K}) \leftarrow Kyber.Encap(\hat{pk})$				
$\hat{K} \leftarrow Kyber.Decap(\hat{sk},\hat{c})$		$C_2 := IC_2.Enc(rw, \hat{c})$				
$K_0 := G(C^{(i)}, S^{(j)}, C_1, C_2, \hat{K})$		$K_0 := G(C^{(i)}, S^{(j)}, C_1, C_2, \hat{K})$				
$c \leftarrow AE_{it}.Dec(H_2(K_0),\psi)$		$(c, K_1) \leftarrow Kyber.Encap(pk)$				
Abort if $c = \bot$	$C_2, \left[\psi ight]$	$\psi \leftarrow AE_{it}.Enc(H_2(K_0),c)$				
$r := H_1(pw, C^{(i)}, S^{(j)})$	<i>\</i>					
$(pk, sk) \leftarrow Kyber.KeyGen(r)$						
$K_1 \leftarrow Kyber.Decap(sk,c)$	$[\sigma]$	$sid := C_1   C_2$				
$sid := C_1   C_2$	$\longrightarrow$	Abort if $\sigma \neq H_3(K_0, K_1, sid \psi)$				
$\sigma := H_3(K_0, K_1, sid \psi)$		$sKey := H_4(K_0)$				
$sKey := H_4(K_0)$		L				

Fig. 9: The Kyber-based aPAKE scheme resulting from compiling the Kyber-based PAKE in [2] with our Kyber-based compiler. The dashed part is our Kyber-based compiler. Kyber = (Kyber.KeyGen, Kyber.Encap, Kyber.Decap) denotes the CCA-secure Kyber.

In the following, we also recall the definition of the MDDH assumption and present the MDDH-based OW-ChCCA KEM scheme proposed in [26] in Fig. 10. In the MDDH-based KEM scheme, we use [a] to represent a group element  $g^a$  and naturally extend to vectors  $[\mathbf{v}]$  and matrices  $[\mathbf{A}]$ . The UC-security of the CDH-based PAKE scheme in [22] is recalled in Lemma 2.

**Definition 7 (Matrix DDH Assumption [13]).** Let  $k \in \mathbb{N}$  and GGen is a group generation algorithm that outputs  $(\mathbb{G}, g, p)$  on input  $1^{\lambda}$ . The k-MDDH assumption holds, if for any PPT  $\mathcal{A}$ , we have

$$\mathsf{Adv}_{\mathsf{MDDH}}(\mathcal{A}) := \left| \Pr\left[\mathcal{A}(\mathbb{G}, g, p, [\mathbf{A}], [\mathbf{b}]) \Rightarrow 1\right] - \Pr\left[\mathcal{A}(\mathbb{G}, g, p, [\mathbf{A}], [\mathbf{u}]) \Rightarrow 1\right] \right| = \mathsf{negl}(\lambda)$$

 $where \ (\mathbb{G},g,p) \leftarrow \mathsf{GGen}, \mathbf{A} \leftarrow_{\$} \mathbb{Z}_p^{(k+1) \times k}, \mathbf{x} \leftarrow_{\$} \mathbb{Z}_p^k, \mathbf{b} := \mathbf{A}\mathbf{x}, \mathbf{u} \leftarrow_{\$} \mathbb{Z}_p^{k+1}.$ 

**Lemma 2** ([26], Theorem 4). The KEM scheme in Fig. 10 is tightly OW-ChCCA secure. Concretely, for any PPT adversary A, for any  $N = poly(\lambda)$  and  $\ell = \mathsf{poly}(\lambda), \text{ there exists a PPT algorithm } \mathcal{B} \text{ such that}$ 

$$\mathsf{Adv}_{\mathsf{KEM}}^{(N,\ell)-\mathsf{ChCCA}} \leq 12 \cdot \mathsf{Adv}_{\mathsf{MDDH}}(\mathcal{B}) + 2^{-\Omega(\lambda)}.$$

**Lemma 3 ([22], Theorem 2).** The PAKE scheme in Fig. 11 securely emulates  $\mathcal{F}_{pake}$ . Concretely, we have

 $\left|\Pr\left[\mathbf{Real}_{\mathcal{Z},\mathcal{A}}\right] - \Pr\left[\mathbf{Ideal}_{\mathcal{Z},\mathsf{Sim}}\right]\right| \le 2 \cdot \mathsf{Adv}_{\mathsf{CDH}}(\mathcal{B}) + 2^{-\Omega(\lambda)}.$ 

Finally, when applying our MDDH-based compiler to the tightly UC-secure PAKE scheme [22], we obtain the first tightly UC-secure aPAKE scheme, as shown in Fig. 11.

$Setup(1^{\lambda})$ :	Decap(sk,c):
$\boxed{(\mathbb{G},p,g)} \leftarrow GGen(1^{\lambda})$	Parse $c = (C_0, C_1, [\mathbf{x}], \hat{h}_0, \hat{h}_1))$
$[\mathbf{A}] \leftarrow_{\$} \mathbb{G}^{3  imes 3}$	Parse $sk = (\mathbf{z}_b, b)$
Return $pp := (\mathbb{G}, p, g, [\mathbf{A}])$	$h'_b := \hat{h}_b \oplus [\mathbf{z}_{\mathbf{b}}^\top \mathbf{x}] \in \{0, 1\}^{\log p}$
	$\hat{K}_b := H([\mathbf{x}], \hat{h}_b, h'_b)$
KeyGen(pp)	$R := C_b \oplus \hat{K}_b$
$b \leftarrow \{0,1\}, \mathbf{z}_b \leftarrow \mathbb{Z}_p^3$	$(\mathbf{s}, h_0, h_1) := G(R)$
$[\mathbf{u}_b] := [\mathbf{A}\mathbf{z}_b], [\mathbf{u}_{1-b}] \leftarrow_{\mathrm{s}} \mathbb{G}^3$	$\hat{h}'_{1-b} := [\mathbf{s}^\top \mathbf{u}_{1-b}] \oplus h_1$
$pk := ([\mathbf{u}_0], [\mathbf{u}_1]), sk := (\mathbf{z}_b, b)$	$\hat{K}_{1-b} := H([\mathbf{x}], \hat{h}'_{1-b}, h_{1-b})$
	If $\mathbf{x} \neq [\mathbf{A}^{\top}\mathbf{s}]$ : return $\perp$
$\frac{Encap(pk):}{Encap(pk)}$	If $\hat{K}_{1-b} \oplus R \neq C_{1-b}$ : return $\perp$
$R \leftarrow \{0,1\}^{\lambda}, (\mathbf{s}, h_0, h_1) := G(R)$	If $h'_b \neq h_b$ : return $\perp$
$\begin{bmatrix} \mathbf{x} \end{bmatrix} := \begin{bmatrix} \mathbf{A}^\top s \end{bmatrix} \in \mathbb{G}^3$	If $\hat{h}'_{1-b} \neq \hat{h}_{1-b}$ : return $\perp$
$\hat{h}_0 := [\mathbf{s}^\top \mathbf{u}_0] \oplus h_0 \in \{0, 1\}^{\log p}$	return $K := R$
$\hat{h}_1 := [\mathbf{s}^\top \mathbf{u}_1] \oplus h_1 \in \{0, 1\}^{\log p}$	
$\hat{K}_0 := H([\mathbf{x}, \hat{h}_0, h_0]), C_0 := \hat{K}_0 \oplus R$	
$\hat{K}_1 := H([\mathbf{x}, \hat{h}_1, h_1]), C_1 := \hat{K}_1 \oplus R$	
$c := (C_0, C_1, [\mathbf{x}], \hat{h}_0, \hat{h}_1)$	
return $(c, K := R)$	

Fig. 10: The MDDH based OW-ChCCA secure KEM scheme in [26].

• $KEM_{MDDH} := (KEM_{MDDH}.KeyGen, KEM_{MDDH}.Encap, KEM_{MDDH}.Decap)$						
• A group $(\mathbb{G}, g, p)$ .						
• Two ideal ciphers $IC_1$ on domain $\mathbb{G} \times \mathbb{G}$ and $IC_2$ on domain $\mathbb{G}$ .						
• Hash functions $H_0, H_2, H_3, G: \{0,1\}^* \to \{0,1\}^{\lambda}$ ,						
		e of KEM <sub>MDDH</sub> .KeyGen				
<u>Client <math>C^{(i)}</math></u> :		Server $S^{(j)}$ :				
	Registration					
on input $pw$ :						
$\overline{rw} := H_0(pw, C^{(i)}, S^{(j)});$						
$r := H_1(pw, C^{(i)}, S^{(j)})$	rw, pk					
$(pk, sk) \leftarrow KEM_{MDDH}.KeyGen(r)$	/	store $(rw, pk)$				
	Login					
on input $pw$ :		on input $(rw, pk)$ :				
$\overline{x_1, x_2 \leftarrow \mathbb{S} \mathbb{Z}_p}, X_1 := g^{x_1}, X_2 := g^{x_2}$						
$e_1 \leftarrow IC_1.Enc(H_0(pw), X_1 X_2)$	$e_1$	$y \leftarrow \mathbb{Z}_p, Y := g^y$				
	$\longrightarrow$	$e_2 \leftarrow IC_2.Enc(rw,Y)$				
$Y \leftarrow IC_2.Dec(H_0(pw), e_2)$		$X_1 X_2 \leftarrow IC_1.Dec(rw, e_1)$				
$sid := C S e_1 e_2$		$sid := C S e_1 e_2$				
$K_0 := G(sid, Y^{x_1}, Y^{x_2}, pw)$		$K_0 := G(sid, X_1^y, X_2^y, pw)$				
$c \leftarrow AE_{it}.Dec(H_2(K_0),\psi)$	$e_2, [\psi]$	$(c, K_1) \leftarrow KEM_{MDDH}.Encap(pk)$				
Abort if $c = \bot$	$\leftarrow$	$\psi \leftarrow AE_{it}.Enc(H_2(K_0),c)$				
$r := H_1(pw, C^{(i)}, S^{(j)})$						
$(pk, sk) \leftarrow KEM_{MDDH}.KeyGen(r))$						
$K_1 \leftarrow KEM_{MDDH}.Decap(sk,c)$		Abort if $\sigma := H_3(K_0, K_1, sid \psi)$				
$\sigma := H_3(K_0, K_1, sid \psi)$	$\xrightarrow{[\sigma]}$	$sKey := H_4(K_0)$				
$sKey := H_4(K_0)$	,					

Fig.11: The tightly secure MDDH-based aPAKE scheme resulting from compiling the CDH-based PAKE in [22] with our KEM-based compiler. The dashed part is our KEM-based compiler installed with  $\mathsf{KEM}_{\mathsf{MDDH}} = (\mathsf{KEM}_{\mathsf{MDDH}}.\mathsf{KeyGen},\mathsf{KEM}_{\mathsf{MDDH}}.\mathsf{Encap},\mathsf{KEM}_{\mathsf{MDDH}}.\mathsf{Decap})$  shown in Fig. 10, which is a tightly secure OW-ChCCA secure KEM scheme in [26].

# Table of Contents

Ef	ficient Asymmetric PAKE Compiler from KEM and AE	1
	You Lyu <sup>®</sup> , Shengli Liu <sup>(⊠)</sup> <sup>®</sup> , and Shuai Han <sup>®</sup>	
1	Introduction	1
2	Preliminary	10
	2.1 KEM and AE	10
	2.2 Idealized Random Oracle Model	12
	2.3 (Asymmetric) PAKE under UC Framework	12
3	Our aPAKE Compiler from KEM and AE	15
4	Instantiations of aPAKE from Our Compiler and PAKE	27
	4.1 Most Efficient aPAKE from Lattice	28
	4.2 Tightly Secure aPAKE Scheme from Matrix DDH	29
Α	Full Descriptions of Simulator Sim	33
В	Proof of Theorem 2: Tight Reduction for Our aPAKE Compiler	
	from OW-ChCCA Secure KEM	35
С	Proof of Lemma 1: Security Proof for the Information-Theoretic AE	
	Scheme	38
D	Comparison with Other aPAKE Compilers from Post-quantum	
	Assumptions	39
Е	Concrete aPAKE Schemes	39
	E.1 Kyber-Based aPAKE Scheme from Lattices	39
	E.2 Tightly UC-Secure aPAKE Scheme from MDDH	39