Key Encapsulation Mechanisms from Extractable Hash Proof Systems, Revisited

Takahiro Matsuda and Goichiro Hanaoka

Research Institute for Secure Systems,
National Institute of Advanced Industrial Science and Technology (AIST), Japan
{t-matsuda,hanaoka-goichiro}@aist.go.jp

Abstract. In CRYPTO 2010, Wee proposed the notion of "extractable hash proof systems" (XHPS), and its richer version, "all-but-one XHPS" (ABO-XHPS), and showed that chosen ciphertext secure (CCA secure) key encapsulation mechanisms (KEM) can be constructed from them. This elegantly explains several recently proposed practical KEMs constructed based on the "all-but-one" simulation paradigm in a unified framework. Somewhat frustratingly, however, there still exist popular KEMs whose construction and security proofs are not captured by this framework. In this paper, we revisit the framework of the ABO-XHPS-based KEM. Firstly, we show that to prove CCA security of the ABO-XHPS-based KEM, some requirements can be relaxed. This relaxation widens the applicability of the original framework, and explains why many known practical KEMs can be proved CCA secure. Moreover, we introduce new properties for ABO-XHPS, and show how one of the properties leads to KEMs that achieve "constrained" CCA security, which is a useful security notion of KEMs for obtaining CCA secure public key encryption via hybrid encryption. Thirdly, we investigate the relationships among computational properties that we introduce in this paper, and derive a useful theorem that enables us to understand the structure of KEMs of a certain type in a modular manner. Finally, we show that the ABO-XHPS-based KEM can be extended to efficient multi-recipient KEMs. Our results significantly extend the framework for constructing a KEM from ABO-XHPS, enables us to capture and explain more existing practical CCA secure schemes (most notably those based on the decisional Diffie-Hellman assumption) in the framework, and leads to a number of new instantiations of (single- and multi-recipient) KEMs.

Keywords: key encapsulation mechanism, extractable hash proof system, chosen ciphertext security, constrained chosen ciphertext security.

1 Introduction

Background and Motivation. Studies on constructing and understanding practical public key encryption (PKE) schemes secure against chosen ciphertext attacks (CCA security) [24,9] are important research themes in the area of cryptography. Among several approaches towards practical CCA secure PKE schemes, the promising approach is to construct a PKE scheme via the hybrid encryption methodologies using a key encapsulation mechanism (KEM) and a data encapsulation mechanism (DEM). Cramer and

K. Kurosawa and G. Hanaoka (Eds.): PKC 2013, LNCS 7778, pp. 332–351, 2013.

Shoup [8] show that if we combine a CCA secure KEM and a CCA secure DEM, then we obtain a hybrid PKE scheme which is CCA secure. Hofheinz and Kiltz [17] introduce a security notion called *constrained CCA* security (CCCA security), and show that a CCA secure PKE scheme can be constructed by combining a CCCA secure KEM and a DEM satisfying the security of (one-time) authenticated encryption [2]. These results enable us to concentrate on studying practical constructions of (C)CCA secure KEMs, for obtaining practical PKE schemes.

Seeing in a larger perspective, there are two general paradigms towards CCA secure PKE schemes: the first paradigm uses non-interactive proofs of "well-formedness" [10], which includes the constructions with non-interactive zero-knowledge proofs [22,9,25] that cover generic constructions from cryptographic primitives, and the constructions with *universal hash proof systems* [7,17] that cover practical and efficient schemes based on specific intractability of decision problems.; The second paradigm uses the so-called "all-but-one" simulation technique, (e.g. [3,5,19,17,23,12,18,27]). In fact, [9] can also be seen to be included in this paradigm. These two paradigms in fact cover almost all known constructions of CCA secure PKE schemes and KEMs. Our focus in this paper is on KEMs constructed based on the second paradigm.

In CRYPTO'10, Wee [27] introduced the notion of "*extractable hash proof systems*" (XHPS) and its richer version "*all-but-one XHPS*" (ABO-XHPS), which are both a special kind of non-interactive proof system for a family of *one-way relations* (which defines a hard search problem, such as the computational Diffie-Hellman problem), and showed that CCA secure KEMs can be constructed from them. This framework elegantly explains the constructions and the security proofs of several (variants of) recently proposed KEMs (e.g. [6,18]) based on hardness of "search" problems (not only "decision" problems), which are proved with the "all-but-one" simulation paradigm.

Somewhat frustratingly, however, there still exist several popular KEMs (e.g. [17,6,12]) whose construction and (C)CCA security are not explained by the framework in [27], although those that cannot be explained by the framework in [27] are quite similar to those that can be explained. The main motivation of this work is to extend the framework of KEMs based on ABO-XHPS to capture a wider class of constructions and security proofs of CCA secure, and even CCCA secure, KEMs, so that it works as a more general framework capturing a wider class of constructions based on the "all-but-one" simulation paradigm as we categorized above. Such general framework can be expected to lead to deeper understanding of constructions and security proofs of KEMs and be useful for future design of (C)CCA secure practical KEMs and PKE schemes, and higher level primitives/protocols that use those as building blocks.

Our Contribution. In this paper, we revisit and extend the framework for constructing a KEM based on ABO-XHPS in [27] in several different aspects:

Firstly, we show that to prove CCA security of the ABO-XHPS-based KEM, some requirement of ABO-XHPS and its associated one-way relation family can be relaxed. More specifically, the original definition of an ABO-XHPS in [27] requires some unnecessarily strong "correctness" requirement and a underlying one-way relation family with which the ABO-XHPS is associated needs to satisfy "*gap*"-type one-wayness, which requires that one-wayness holds even in the presence of the decision oracle, and thus is a stronger type of one-wayness. Instead, we show that as long as the ABO-XHPS satisfies the property which we call *computational soundness* (CS security, for short), the ABO-XHPS-based KEM can be shown to be CCA secure with a weaker correctness requirement for the underlying ABO-XHPS and a weaker (non-gap) one-way relation. (The formal definitions of an ABO-XHPS and a family of one-way relations are given in Section 3.) Due to these relaxations, we can treat a wider class of computational assumptions, and the class of CCA secure KEMs that can be captured by the framework becomes significantly wider. Most notably, we can now treat the decisional Diffie-Hellman (DDH) assumption as a one-way relation family, and thus several practical DDH-based KEMs (e.g. [6,12]), which was not possible by the original framework because of the requirement of the "gap"-type one-wayness.

Secondly, we propose another computational property of ABO-XHPS which we call "*pseudorandom extraction property*" (PR-Ext security, for short), and show that if an ABO-XHPS satisfies the property, then the ABO-XHPS-based KEM achieves CCCA security. This result enables us to explain CCCA security of the KEMs whose construction and security proof can be understood in the "all-but-one" simulation paradigm. This enables us to cast CCCA secure KEMs proposed in [17] and in [13, Sect. 6] in our extended framework.

Thirdly, we study the computational properties of ABO-XHPS themselves. Specifically, we introduce yet another computational property which we call *weak computational soundness* (wCS security, for short), and show that wCS security is implied by both CS security and PR-Ext security. Furthermore, we show how to combine a PR-Ext secure ABO-XHPS and a wCS secure ABO-XHPS to obtain a CS secure ABO-XHPS. This "transformation," together with the above mentioned results, enables us to understand the constructions and CCA security of KEMs in a modular manner. For example, this provides us with an alternative security proof of the Cash et al. KEM [6, Sect. 5.2], without the "trapdoor test" theorem [6, Theorem 2] that was originally used to prove its CCA security. Moreover, combined with the above mentioned results, this result enables us to derive a number of new variants of KEMs [8,19,17,6,12] that can be shown to be CCA secure under the DDH or the Hashed DH (HDH) assumption [11].

Finally, we show that the ABO-XHPS-based KEM can be extended to be a multi-recipient KEM (MR-KEM) [26,16]. Here, by MR-KEM we mean the one formalized by Smart [26] in which all recipients recover a same session-key. (This differs from multi-recipient PKE by Bellare et al. [1] in which each receiver may recover different message.) From this result, we derive a number of new practical (C)CCA secure MR-KEMs.

The results in this paper are summarized in Fig. 1. Our results enable us to capture more existing practical CCA secure schemes than the original framework [27], derive a number of new practical instantiations of (C)CCA secure (MR-)KEMs, and understand the structures and security proofs of these schemes. (See Section 6 for more details.) We believe that the framework of ABO-XHPS extended by our results widely captures the constructions of KEMs based on the "all-but-one" simulation paradigm and leads to deeper understanding of the constructions and security proofs of practical KEMs, and is useful for future design of (C)CCA secure practical (MR-)KEMs.

Due to space limitations, the full proofs of the theorems in this paper will be given in the full version. We instead give intuitive explanations for each theorem.

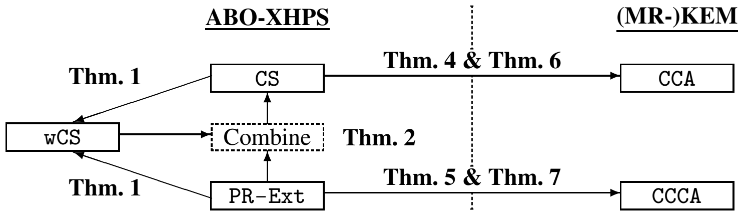

Fig. 1. Summary of our results. Each box with label "X" denotes an X-secure primitive. The arrow (X → Y) indicates that an X-secure primitive can be used to construct a Y-secure primitive.

Related Work. The relevant general framework of constructions of PKE schemes and KEMs is be the framework using *universal hash proof systems* introduced by Cramer and Shoup [7]. This framework, as we mentioned above, can be seen as one of the general paradigms using non-interactive proof of "well-formedness", and captures a wide class of practical constructions of PKE schemes and KEMs, such as Cramer-Shoup PKE scheme [8]. Kurosawa and Desmedt [20] showed how to construct CCA secure KEM directly from hash proof systems. The requirements in the original definition of a universal hash proof system in [7] (and in [20]) were all statistical (information-theoretic) ones. Hofheinz and Kiltz [17] introduced computational relaxation for a universal hash proof system, and showed that the KEM based on a hash proof system in [20] can be shown to be CCCA secure if the underlying hash proof system satisfies some computational property.

Wee [28] recently proposed the notion of *threshold extractable hash proof system*, which can be seen as a generalization of an ABO-XHPS, from "all-but-one" to "all-but-t." From it, he showed how to construct threshold signature schemes, threshold encryption schemes, and broadcast encryption schemes.

2 Preliminaries

In this section, we review the basic notation and the definitions for a (multi-recipient) KEM. Due to space limitation, the definitions for other basic primitives and computational intractability assumptions will be given in the full version.

Basic Notation. $\mathbb{N}$ denotes the set of all natural numbers, and if $n \in \mathbb{N}$ then $[n] = \{1, \dots, n\}$. "$x \leftarrow y$" denotes that x is chosen uniformly at random from y if y is a finite set, or y is assigned to x otherwise. If S is a set, then "$|S|$" denotes its size. "PPTA" denotes a *probabilistic polynomial time algorithm*. Unless otherwise stated, k denotes the security parameter. If $\mathcal{A}$ is an algorithm and $\mathcal{O}$ is a function, then "$\mathcal{A}^{\mathcal{O}}$" denotes that $\mathcal{A}$ has oracle access to $\mathcal{O}$. A function $f(k) : \mathbb{N} \rightarrow [0, 1]$ is said to be *negligible* if for all positive polynomials $p(k)$ and all sufficiently large $k \in \mathbb{N}$, we have $f(k) < 1/p(k)$.

Multi-Recipient KEM. Here, we review the definition of a multi-recipient KEM (MR-KEM). We use the definition formalized by Smart [26], where all recipients recover a same session-key. A MR-KEM Γ consists of the following five PPTAs:

MSetup**:** The setup algorithm that takes 1^k as input, and outputs a set of public parameters pub. pub specifies the session-key space $\mathcal{K}$.

MKG**:** The (user's) key generation algorithm that takes pub as input, and outputs a public/secret key pair (pk, sk). Without loss of generality, we assume that the information on pub is contained in pk and sk, and we do not write pub for the inputs of the following algorithms.

MEnc**:** The encapsulation algorithm that takes a set of public keys $\mathbf{pk} = (pk_1, \dots, pk_n)$ as input, and outputs a ciphertext c and a session-key $K \in \mathcal{K}$.

MExt**:** The (deterministic) user's ciphertext extraction algorithm that takes a user i's public key pk_i, and a ciphertext c (which is output from MEnc) as input, and outputs the user i's ciphertext c_i.

MDec**:** The (deterministic) decapsulation algorithm that takes a user i's secret key sk_i and a user i's ciphertext c_i as input, and outputs a session-key K which could be a special symbol $\perp$ meaning "invalid".

We say that a MR-KEM satisfies *correctness* (resp. *almost-correctness*), if for all $\mathsf{pub} \leftarrow \mathsf{MSetup}(1^k)$ and all polynomials $n = n(k)$, the following probability is zero (resp. negligible).

$$\Pr[\ (pk_i, sk_i) \leftarrow \mathsf{MKG}(\mathsf{pub}) \text{ for } i \in [n];\ (c, K) \leftarrow \mathsf{MEnc}(\mathbf{pk} = (pk_1, \dots, pk_n)) : \\ \mathsf{MDec}(sk_i, \mathsf{MExt}(pk_i, c)) \neq K \text{ for some } i \in [n]\ ]$$

Security Notions. Here, we recall the definitions of indistinguishability against chosen ciphertext attacks (CCA security) and against constrained chosen ciphertext attacks (CCCA security) [17].

Let $\mathtt{ATK} \in \{\mathtt{CCA}, \mathtt{CCCA}\}$ and $n \in \mathbb{N}$. For a MR-KEM $\Gamma = (\mathsf{MSetup}, \mathsf{MKG}, \mathsf{MEnc}, \mathsf{MExt}, \mathsf{MDec})$, we define the experiment $\mathsf{Expt}^{\mathtt{ATK}}_{\Gamma,\mathcal{A},n}(k)$ that an adversary $\mathcal{A}$ attacks Γ under the attack type ATK as follows:

$$\mathsf{Expt}^{\mathtt{ATK}}_{\Gamma,\mathcal{A},n}(k) : [\ \mathsf{pub} \leftarrow \mathsf{MSetup}(1^k);\ (pk_i, sk_i) \leftarrow \mathsf{MKG}(\mathsf{pub}) \text{ for } i \in [n]; \\ \mathbf{pk} \leftarrow (pk_1, \dots, pk_n);\ (c^*, K_1^*) \leftarrow \mathsf{MEnc}(\mathbf{pk});\ K_0^* \leftarrow \mathcal{K};\ b \leftarrow \{0,1\}; \\ b' \leftarrow \mathcal{A}^{\mathcal{O}}(\mathsf{pub}, \mathbf{pk}, c^*, K_b^*);\ \text{If } b' = b \text{ then return } 1 \text{ else return } 0\ ],$$

where the oracle $\mathcal{O}$ is determined by ATK in the following ways: If $\mathtt{ATK} = \mathtt{CCA}$, then the oracle $\mathcal{O}$ is the decapsulation oracle $\mathcal{O}(\cdot,\cdot)$ which takes a user index/ciphertext pair (i, c) as input, and outputs the result of $\mathsf{tMDec}(sk_i, \mathsf{MExt}(pk_i, c))$. If $\mathtt{ATK} = \mathtt{CCCA}$ then the oracle $\mathcal{O}$ is the *constrained decapsulation (CDEC) oracle* $\mathcal{O}_{cdec}(\cdot,\cdot,\cdot)$, which takes a user index i, a predicate $\mathsf{pred} : \mathcal{K} \rightarrow \{0,1\}$, and a ciphertext c as input, and outputs a response that is calculated as follows:

$$\mathcal{O}_{cdec}(i, \mathsf{pred}, c) = \begin{cases} K & \text{If } \mathsf{MDec}(sk_i, \mathsf{MExt}(pk_i, c)) = K \neq \perp \wedge \mathsf{pred}(K) = 1 \\ \perp & \text{Otherwise} \end{cases}$$

Moreover, in both cases $\mathtt{ATK} \in \{\mathtt{CCA}, \mathtt{CCCA}\}$, $\mathcal{A}$ is not allowed to submit a query that contains a user index/ciphertext pair (i, c) satisfying $\mathsf{MExt}(pk_i, c) = \mathsf{MExt}(pk_i, c^*)$ to the oracle.

Let $\mathcal{A}$ be an adversary that runs in a $\mathtt{CCCA}$ experiment and makes in total q queries, and let $(i_j, \mathsf{pred}_j, c_j)$ be $\mathcal{A}$'s j-th CDEC query. "*The running time of* $\mathcal{A}$ *in the* $\mathtt{CCCA}$ *experiment*" is defined as the sum of $\mathcal{A}$'s running time and the total of the maximum running time for evaluating each pred_j submitted by $\mathcal{A}$. "*The running time of the* $\mathtt{CCCA}$ *experiment*" is defined as the total running time of $\mathsf{Expt}^{\mathtt{CCCA}}_{\Gamma,\mathcal{A}}(k)$ minus "the running time of $\mathcal{A}$ in the $\mathtt{CCCA}$ experiment." For a $\mathtt{CCCA}$ adversary $\mathcal{A}$ and an experiment $\mathcal{E}$ (not necessarily $\mathsf{Expt}^{\mathtt{CCCA}}_{\Gamma,\mathcal{A}}(k)$) that $\mathcal{A}$ runs in, we define the parameter called (plaintext) *uncertainty* $\mathsf{uncert}_{\mathcal{A},\mathcal{E}}(k)$ by:

$$\mathsf{uncert}_{\mathcal{A},\mathcal{E}}(k) = \frac{1}{q}\sum_{j\in[q]} \Pr[\mathcal{E}; K \leftarrow \mathcal{K} : \mathsf{pred}_j(K) = 1].$$

Finally, we say that an adversary $\mathcal{A}$ is a *valid* $\mathtt{CCCA}$ *adversary* if (1) "the running time of $\mathcal{A}$ in the $\mathtt{CCCA}$ experiment" is polynomial in k, and (2) $\mathsf{uncert}_{\mathcal{A},\mathcal{E}}(k)$ is negligible for all experiments $\mathcal{E}$ whose running time is at most that of "the running time of the $\mathtt{CCCA}$ experiment" that $\mathcal{A}$ runs in.

For a KEM Γ, an adversary $\mathcal{A}$, $\mathtt{ATK} \in \{\mathtt{CCA}, \mathtt{CCCA}\}$, and $n \in \mathbb{N}$ we define $\mathtt{ATK}$ advantage $\mathsf{Adv}^{\mathtt{ATK}}_{\Gamma,\mathcal{A},n}(k)$ of $\mathcal{A}$ by $\mathsf{Adv}^{\mathtt{ATK}}_{\Gamma,\mathcal{A},n}(k) = |\Pr[\mathsf{Expt}^{\mathtt{ATK}}_{\Gamma,\mathcal{A},n}(k) = 1] - 1/2|$.

Definition 1. *We say that a MR-KEM* Γ *is* $\mathtt{CCA}$ *secure if* $\mathsf{Adv}^{\mathtt{CCA}}_{\Gamma,\mathcal{A},n}(k)$ *is negligible for any PPTA* $\mathcal{A}$ *and any polynomial* $n = n(k)$. *Furthermore, we say that a MR-KEM* Γ *is* $\mathtt{CCCA}$ *secure if* $\mathsf{Adv}^{\mathtt{CCCA}}_{\Gamma,\mathcal{A},n}(k)$ *is negligible for any valid* $\mathtt{CCCA}$ *adversary* $\mathcal{A}$ *and any polynomial* $n = n(k)$.

Single-Recipient KEM. When we talk about ordinary "single-recipient" KEMs, we need not consider the setup and user key generation algorithms separately. Therefore, in order to clarify the difference between multi-recipient KEMs and ordinary KEMs, we write the key generation, the encapsulation, and the decapsulation algorithms of a single-recipient KEM by KG, Enc, and Dec, respectively (without the prefix "M"). The syntax and the security notions for single-recipient KEMs are defined similarly to those of MR-KEMs.

3 Definitions for All-But-One Extractable Hash Proof Systems

In this section, we define an ABO-XHPS and one-way relations which are necessary for ABO-XHPS, following the definitions in [27]. However, our definitions here are slightly different from ones in [27], and we also highlight the difference.

3.1 One-Way Relation Families

A family of relations (relation family, for short) $\mathcal{R}$ (that supports a PRG) is associated with the following three PPTAs (RSetup, RSamp, G):

RSetup**:** The setup algorithm that takes 1^k as input, and outputs a public/private parameter pair $(\mathsf{pub}, \mathsf{pri})$. pub contains the description of sets $\mathcal{U}$, $\mathcal{S}$, $\mathcal{W}$, and $\mathcal{K}$, from which we can efficiently sample elements uniformly. pub also fixes one relation

$\mathcal{R}_{\mathsf{pub}}$ over $\mathcal{U} \times \mathcal{S}$. We require that: (1) for all u, there is at most one s such that $(u, s) \in \mathcal{R}_{\mathsf{pub}}$ (with overwhelming probability over the choice of pub), and (2) given pri (corresponding to pub) and $(u, s) \in \mathcal{U} \times \mathcal{S}$, whether $(u, s) \in \mathcal{R}_{\mathsf{pub}}$ or not is efficiently decidable. For notational convenience, we assume that pub is provided as input to the following algorithms, and do not write it explicitly.

RSamp: The sampling algorithm that (takes pub as input, and) outputs a pair $(u, s) \in \mathcal{R}_{\mathsf{pub}}$ so that u is distributed uniformly over $\mathcal{U}$. The randomness space of RSamp is $\mathcal{W}$, and when we need to make the randomness used to sample (u, s) explicit, we write this process as "$(u, s) \leftarrow \mathsf{RSamp}(w)$" (in this case, RSamp is treated as a deterministic algorithm).

G: The (pseudorandom) generator that takes (pub and) an element $s \in \mathcal{S}$ as input, and outputs $K \in \mathcal{K}$.

Hereafter, we identify a relation family $\mathcal{R}$ with the associated PPTAs (RSetup, RSamp, G), and in particular, write $\mathcal{R} = (\mathsf{RSetup}, \mathsf{RSamp}, \mathsf{G})$.

Definition 2. *We say that* $\mathcal{R} = (\mathsf{RSetup}, \mathsf{RSamp}, \mathsf{G})$ *is a* one-way relation family *if the advantage* $\mathsf{Adv}^{\mathtt{PRG}}_{\mathcal{R},\mathcal{A}}(k)$ *defined below is negligible for any PPTA* $\mathcal{A}$*:*

$$\mathsf{Adv}^{\mathtt{PRG}}_{\mathcal{R},\mathcal{A}}(k) = |\Pr[(\mathsf{pub}, \mathsf{pri}) \leftarrow \mathsf{RSetup}(1^k); (u, s) \leftarrow \mathsf{RSamp};$$
$$K_1^* \leftarrow \mathsf{G}(s); K_0^* \leftarrow \mathcal{K}; b \leftarrow \{0,1\}; b' \leftarrow \mathcal{A}(\mathsf{pub}, u, K_b^*) : b' = b] - \frac{1}{2}|.$$

Furthermore, we say that $\mathcal{R}$ *is a* gap one-way relation family *if the advantage is negligible for any PPTA adversary that is given access to the "relation" oracle which takes* $(u, s) \in \mathcal{U} \times \mathcal{S}$ *as input and tells if* $(u, s) \in \mathcal{R}_{\mathsf{pub}}$ *or not.*

Difference from the Definition in [27]. The original definition of one-way relation families in [27] is the "gap" version here. The definition of (non-gap-)one-way relation family is clearly weaker, thus potentially easier to achieve and captures wider class of relation families than the gap version. For example, the "gap" one-way relation of [27] does not capture the HDH-based Diffie-Hellman relation family we introduce below.[1]

Concrete Example of One-Way Relation Families: Diffie-Hellman Relation. Let $\mathbb{G}$ be a group of prime order p and let $H : \mathbb{G} \to \mathcal{K}$ be a hash function. We say that the hashed Diffie-Hellman (HDH) assumption holds in $(\mathbb{G}, H)$ if the distributions of $(g, g^a, g^b, H(g^{ab}))$ and (g, g^a, g^b, K) are computationally indistinguishable, where $g \in \mathbb{G}$, $a, b \in \mathbb{Z}_p$, and $K \in \mathcal{K}$ are chosen randomly.[2]

The Diffie-Hellman relation family (that supports a PRG H) $\mathcal{R}^{\mathsf{DH}}$, indexed by $\mathsf{pub} = (g, g^\alpha) \in (\mathbb{G})^2$, is defined by $\mathcal{R}^{\mathsf{DH}}_{(g,g^\alpha)} = \{(u, s) \in (\mathbb{G})^2 | s = u^\alpha\}$. The associated algorithms (RSetup, RSamp, G) are as follows: RSetup sets $\mathcal{U} = \mathcal{S} = \mathbb{G}$ and $\mathcal{W} = \mathbb{Z}_p$,

[1] We note that in [28], Wee introduced the definition of one-way relation families in the same sense as the one defined here.

[2] The DDH assumption is the special case of the HDH assumption in which H is the identity function. It is possible that the DDH assumption in $\mathbb{G}$ is false while the HDH assumption in $(\mathbb{G}, H)$ holds for some H. For more details about the HDH assumption, see [11,19,6,12] and the full version of this paper.

picks random elements $g \in \mathbb{G}$ and $\alpha \in \mathbb{Z}_p$, and sets $\mathsf{pub} = (g, h) = (g, g^{\alpha})$ and $\mathsf{pri} = \alpha$. $\mathsf{RSamp}(w) := (g^w, h^w)$. $\mathsf{G}(s) := H(s)$. It is straightforward to see that $\mathcal{R}^{\mathsf{DH}}$ is a one-way relation family under the HDH assumption in $(\mathbb{G}, H)$.

3.2 All-But-One Extractable Hash Proof Systems

An ABO-XHPS is always associated with a relation family. Thus, for notational convenience, we denote by "$\mathcal{X}^{\mathcal{R}}$" an ABO-XHPS $\mathcal{X}$ associated with a relation family $\mathcal{R}$. (If $\mathcal{R}$ is clear from the context, we often omit $\mathcal{R}$ and just write $\mathcal{X}$.) Informally, an ABO-XHPS is a special type of "designated-verifier non-interactive zero-knowledge proof of knowledge," and it has, as its internal structure, a family of "tag-based" hash functions $\mathsf{H}_{pk} : \mathcal{T} \times \mathcal{U} \rightarrow \{0,1\}^*$ indexed by a public key pk (where $\mathcal{T}$ is the tag space) which represents the relation of an instance $u \in \mathcal{U}$ and a (tag-based) "proof" $\pi = \mathsf{H}_{pk}(\mathsf{tag}, u)$ (with some $\mathsf{tag} \in \mathcal{T}$). If π is in a valid form, we can "extract" the answer s to the instance u satisfying $(u, s) \in \mathcal{R}_{\mathsf{pub}}$, using the secret key corresponding to pk. It is possible that H itself is not efficiently computable. Furthermore, $\mathcal{X}$ has "simulation" algorithms for key generation, extraction, and generating a proof. The first two algorithms work normally as above, except for one particular tag tag^* (used for the simulated key generation process) under which one can generate a valid proof without a witness (hence the name "all-but-one").

Formally, an ABO-XHPS $\mathcal{X}$, associated with a relation family $\mathcal{R} = (\mathsf{RSetup}, \mathsf{RSamp}, \mathsf{G})$, consists of six PPTAs $(\mathsf{XKG}, \mathsf{Pub}, \mathsf{Ext}, \widehat{\mathsf{XKG}}, \widehat{\mathsf{Priv}}, \widehat{\mathsf{Ext}})$ that satisfy the following "functional requirements" (correctness) with overwhelming probability over the choice of $(\mathsf{pub}, \mathsf{pri}) \leftarrow \mathsf{RSetup}(1^k)$:

Extraction Mode. For all $(pk, sk) \leftarrow \mathsf{XKG}(\mathsf{pub}, \mathsf{pri})$ and all tuples (tag, u, π): If $\pi = \mathsf{H}_{pk}(\mathsf{tag}, u)$ then $(u, \mathsf{Ext}(sk, \mathsf{tag}, u, \pi)) \in \mathcal{R}_{\mathsf{pub}}$, and if $\pi \neq \mathsf{H}_{pk}(\mathsf{tag}, u)$ then $\mathsf{Ext}(sk, \mathsf{tag}, u, \pi) = \bot$.

All-But-One Mode. For all tag^* and all $(pk, \widehat{sk}) \leftarrow \widehat{\mathsf{XKG}}(\mathsf{pub}, \mathsf{tag}^*)$:
Private Evaluation under tag^*: For all $(u, s) \in \mathcal{R}_{\mathsf{pub}}$: $\widehat{\mathsf{Priv}}(\widehat{sk}, u) = \mathsf{H}_{pk}(\mathsf{tag}^*, u)$.
Extraction: For all $\mathsf{tag} \neq \mathsf{tag}^*$ and all (u, π): If $\pi = \mathsf{H}_{pk}(\mathsf{tag}, u)$ then $(u, s) \in \mathcal{R}_{\mathsf{pub}}$, where $s = \widehat{\mathsf{Ext}}(\widehat{sk}, \mathsf{tag}, u, \pi)$. (The case of $\pi \neq \mathsf{H}_{pk}(\mathsf{tag}, u)$ is unspecified.)

Public Evaluation. For all pk (output from either XKG or $\widehat{\mathsf{XKG}}$), tag, and $(u, s) = \mathsf{RSamp}(w)$: $\mathsf{Pub}(pk, \mathsf{tag}, w) = \mathsf{H}_{pk}(\mathsf{tag}, u)$.

Indistinguishability of Two Modes. For all tag^*, the two distributions, $\{(pk, sk) \leftarrow \mathsf{XKG}(\mathsf{pub}, \mathsf{pri}) : pk\}$ and $\{(pk, \widehat{sk}) \leftarrow \widehat{\mathsf{XKG}}(\mathsf{pub}, \mathsf{tag}^*) : pk\}$, are statistically indistinguishable.

In this paper, we also consider a slight relaxation of the extraction property of the "all-but-one" mode. We say that an ABO-XHPS satisfies *almost-correctness* if for all $(\mathsf{pub}, \mathsf{pri}) \leftarrow \mathsf{RSetup}(1^k)$, all $(u, s) = \mathsf{RSamp}(w)$, and all $(\mathsf{tag}, \mathsf{tag}^*)$ such that $\mathsf{tag} \neq \mathsf{tag}^*$, the following probability is overwhelming: $\Pr[(pk, \widehat{sk}) \leftarrow \widehat{\mathsf{XKG}}(\mathsf{pub}, \mathsf{tag}^*) : \widehat{\mathsf{Ext}}(\widehat{sk}, \mathsf{tag}, u, \mathsf{H}_{pk}(\mathsf{tag}, u)) = s]$.

We note that the indistinguishability of the two modes implies that the information on a tag tag^* is statistically hidden from pk output from $\widehat{\mathsf{XKG}}(\mathsf{pub}, \mathsf{tag}^*)$.

Difference from the Definition in [27]. Here, we explain the difference of our definition of ABO-XHPS and the definition by Wee [27, Sect. 3.4]. Firstly, XKG algorithm in [27] does not take the private parameter pri as input (while ours does). However, this restriction is unnecessary for proving (C)CCA security of the ABO-XHPS-based KEM, and thus we allow XKG to take pri as input.

Secondly, the correctness requirements of Ext and $\widehat{\mathsf{Ext}}$ algorithms in [27] are defined in an "if-and-only-if" style. More specifically, the correctness requirements of Ext and $\widehat{\mathsf{Ext}}$ algorithms in [27] are: (i) "$\pi = \mathsf{H}_{pk}(\mathsf{tag}, u) \Leftrightarrow (u, \mathsf{Ext}(sk, \mathsf{tag}, u, \pi)) \in \mathcal{R}_{\mathsf{pub}}$," and (ii) "$\pi = \mathsf{H}_{pk}(\mathsf{tag}, u) \Leftrightarrow (u, \widehat{\mathsf{Ext}}(\widehat{sk}, \mathsf{tag}, u, \pi)) \in \mathcal{R}_{\mathsf{pub}}$." Regarding (i), since the definition of [27] does not specify what is output from Ext when $\mathsf{H}_{pk}(\mathsf{tag}, u) \neq \pi$, we require that it output $\bot$. We stress that this is without loss of generality because given pri, it is possible to tell whether $(u, \mathsf{Ext}(sk, \mathsf{tag}, u, \pi)) \in \mathcal{R}_{\mathsf{pub}}$ or not, and pri can be contained in sk in our definition. The main difference from the definition in this paper and the one in [27] is regarding (ii), i.e. correctness of $\widehat{\mathsf{Ext}}$ algorithm. It is clear that ours requires weaker correctness since we do not specify the behavior of $\widehat{\mathsf{Ext}}$ in case $\mathsf{H}_{pk}(\mathsf{tag}, u) \neq \pi$, while the definition in [27] does. As will be shown later, this relaxation is the main reason that makes the framework of the ABO-XHPS-based KEM much wider, and makes it possible to capture most known practical CCA secure KEMs, and even CCCA secure schemes.

4 Computational Properties of ABO-XHPS

In this section, we introduce three computational properties of ABO-XHPS which are all related to the behavior of the extraction algorithm for the all-but-one mode, i.e. $\widehat{\mathsf{Ext}}$, and play important roles for proving (C)CCA security of the ABO-XHPS-based KEMs in the next section. We also show the relationships among these properties.

4.1 Computational Soundness (CS)

"*Computational soundness*" (CS security) captures soundness of the $\widehat{\mathsf{Ext}}$ algorithm, and roughly means that it is hard to find an "invalid proof" π from which $\widehat{\mathsf{Ext}}$ extracts some value that is not $\bot$. This is, it is hard to find a tuple (tag, u, π) satisfying $\mathsf{tag} \neq \mathsf{tag}^*$, $\mathsf{H}_{pk}(\mathsf{tag}, u) \neq \pi$, and $\widehat{\mathsf{Ext}}(\widehat{sk}, \mathsf{tag}, u, \pi) \neq \bot$, where $(pk, sk) \leftarrow \widehat{\mathsf{XKG}}(\mathsf{pub}, \mathsf{tag}^*)$. Formally, consider the experiment $\mathsf{Expt}^{\mathtt{CS}}_{\mathcal{X},\mathcal{A}}(k)$ that an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ runs in as in Fig. 2 (top-left).

Definition 3. *We say that an ABO-XHPS $\mathcal{X}$ satisfies* computational soundness *(CS secure, for short), if the advantage* $\mathsf{Adv}^{\mathtt{CS}}_{\mathcal{X},\mathcal{A}}(k) = \Pr[\mathsf{Expt}^{\mathtt{CS}}_{\mathcal{X},\mathcal{A}}(k) = 1]$ *is negligible for any PPTA $\mathcal{A}$.*

Concrete CS *Secure ABO-XHPS.* The factoring-based ABO-XHPS [27, Sect. 4.2], the (non-twin-)Diffie-Hellman-based one [27, Sect. 5.1] in case instantiated with bilinear groups, and the twin Diffie-Hellman-based one [27, Sect. 5,2] shown by Wee, are in fact all CS secure. The $\widehat{\mathsf{Ext}}$ algorithm of these ABO-XHPS satisfy the "if-and-only-if"-style

```
$\mathsf{Expt}^{\mathtt{CS}}_{\mathcal{X},\mathcal{A}}(k)$ :
  $(\mathsf{pub}, \mathsf{pri}) \leftarrow \mathsf{RSetup}(1^k)$;
  $(\mathsf{tag}^*, \mathsf{st}) \leftarrow \mathcal{A}_1(\mathsf{pub})$;
  $(pk, \widehat{sk}) \leftarrow \widehat{\mathsf{XKG}}(\mathsf{pub}, \mathsf{tag}^*)$;
  $\mathcal{A}_2^{\mathcal{O}_{\mathtt{CS}}}(pk, \mathsf{st})$;
  If $\mathcal{A}_2$ submits to oracle $\mathcal{O}_{\mathtt{CS}}$
    at least one query
      $(\mathsf{tag}', u', \pi')$ such that
    $\mathsf{tag}' \neq \mathsf{tag}^*$
    $\wedge\ \mathsf{H}_{pk}(\mathsf{tag}', u') \neq \pi'$
    $\wedge\ \widehat{\mathsf{Ext}}(\widehat{sk}, \mathsf{tag}', u', \pi') \neq \perp$
  then return 1 else return 0
```

```
The oracle in $\mathsf{Expt}^{\mathtt{CS}}_{\mathcal{X},\mathcal{A}}(k)$:
$\mathcal{O}_{\mathtt{CS}}(\mathsf{tag}, u, \pi) =$
  $\begin{cases} \widehat{\mathsf{Ext}}(\widehat{sk}, \mathsf{tag}, u, \pi) & \text{If } \mathsf{tag} \neq \mathsf{tag}^* \\ \perp & \text{Otherwise} \end{cases}$

The oracle in $\mathsf{Expt}^{\mathtt{PR\text{-}Ext}}_{\mathcal{X},\mathcal{A}}(k)$ and $\mathsf{Expt}^{\mathtt{wCS}}_{\mathcal{X},\mathcal{A}}(k)$:
$\mathcal{O}_{\mathtt{PR\text{-}Ext}}(\mathsf{tag}, u, \pi) = \mathcal{O}_{\mathtt{wCS}}(\mathsf{tag}, u, \pi) =$
  $\begin{cases} \widehat{\mathsf{Ext}}(\widehat{sk}, \mathsf{tag}, u, \pi) & \text{If } \mathsf{tag} \neq \mathsf{tag}^* \wedge \mathsf{H}_{pk}(\mathsf{tag}, u) = \pi \\ \perp & \text{Otherwise} \end{cases}$
```

```
$\mathsf{Expt}^{\mathtt{PR\text{-}Ext}}_{\mathcal{X},\mathcal{A}}(k)$ :
  $(\mathsf{pub}, \mathsf{pri}) \leftarrow \mathsf{RSetup}(1^k)$;
  $(\mathsf{tag}^*, \mathsf{st}) \leftarrow \mathcal{A}_1(\mathsf{pub})$;
  $(pk, \widehat{sk}) \leftarrow \widehat{\mathsf{XKG}}(\mathsf{pub}, \mathsf{tag}^*)$;
  $(\mathsf{tag}', u', \pi', \mathsf{st}') \leftarrow \mathcal{A}_2^{\mathcal{O}_{\mathtt{PR\text{-}Ext}}}(pk, \mathsf{st})$;
  $s_1' \leftarrow \widehat{\mathsf{Ext}}(\widehat{sk}, \mathsf{tag}', u', \pi')$;
  $s_0' \leftarrow \mathcal{S}$;
  $b \leftarrow \{0, 1\}$;
  $b' \leftarrow \mathcal{A}_3(s_b', \mathsf{st}')$;
  If $b' = b$ then return 1 else return 0
```

```
$\mathsf{Expt}^{\mathtt{wCS}}_{\mathcal{X},\mathcal{A}}(k)$ :
  $(\mathsf{pub}, \mathsf{pri}) \leftarrow \mathsf{RSetup}(1^k)$;
  $(\mathsf{tag}^*, \mathsf{st}) \leftarrow \mathcal{A}_1(\mathsf{pub})$;
  $(pk, \widehat{sk}) \leftarrow \widehat{\mathsf{XKG}}(\mathsf{pub}, \mathsf{tag}^*)$;
  $(\mathsf{tag}', u', \pi', s') \leftarrow \mathcal{A}_2^{\mathcal{O}_{\mathtt{wCS}}}(pk, \mathsf{st})$;
  If $\mathsf{tag}' \neq \mathsf{tag}^*$
    $\wedge\ \mathsf{H}_{pk}(\mathsf{tag}', u') \neq \pi'$
    $\wedge\ s' = \widehat{\mathsf{Ext}}(\widehat{sk}, \mathsf{tag}', u', \pi')$
      $= \widehat{\mathsf{Ext}}(\widehat{sk}, \mathsf{tag}', u', \mathsf{H}_{pk}(\mathsf{tag}', u'))$
  then return 1 else return 0
```

Fig. 2. The CS experiment (top-left), the PR-Ext experiment (bottom-left), the wCS experiment (bottom-right), and the definitions of the oracles (top-right)

correctness, and additionally have the property that invalid proofs $\pi \neq \mathsf{H}_{pk}(\mathsf{tag}, u)$ can be detected publicly or by using a secret key of the ABO-XHPS. Furthermore, the recently proposed practical CCA secure KEMs based on the HDH and the DBDH assumptions can be understood as CS secure ABO-XHPS. These include (a simplified version of) the KEM in [5], [6, Sect. 5.2], and [13, Sect. 4]. Concretely, here we show the ABO-XHPS $\mathcal{X}_{\mathtt{CKS}}$ based on the KEM by Cash et al. [6, Sect. 5.2], which is associated with the HDH-based Diffie-Hellman relation family $\mathcal{R}^{\mathsf{DH}}$, as in Fig. 3. $\mathcal{X}_{\mathtt{CKS}}$ can be proved to be CS secure because the truth value of the validity check in the $\widehat{\mathsf{Ext}}$ algorithm of $\mathcal{X}_{\mathtt{CKS}}$ is the same as the truth value of the validity check in the Ext algorithm with overwhelming probability, due to the "trapdoor test" [6, Theorem 2]. In the full version, we also show ABO-XHPS based on the KEMs in [5] and [13, Sect. 4].

4.2 Pseudorandom Extraction Property (PR-Ext)

The "*pseudorandom extraction property*" (PR-Ext security) guarantees that if the $\widehat{\mathsf{Ext}}$ algorithm is given (tag, u, π) such that $\mathsf{H}_{pk}(\mathsf{tag}, u) \neq \pi$ and $\mathsf{tag} \neq \mathsf{tag}^*$, then the extracted value $s = \widehat{\mathsf{Ext}}(\widehat{sk}, \mathsf{tag}, u, \pi)$ looks pseudorandom. In the context of the ABO-XHPS-based KEMs (that will be shown later), this property means that when $c = (u, \pi)$ is an inconsistent ciphertext, if we extract s from $\widehat{\mathsf{Ext}}$, then the seed s of the session-key

$\mathsf{XKG}(\mathsf{pub} = (g,h), \mathsf{pri} = \alpha)$: $x, y_1, y_2 \leftarrow \mathbb{Z}_p;\ X \leftarrow g^x$ $Y_i \leftarrow g^{y_i}$ for $i \in [2]$ $pk \leftarrow (g, h, X, Y_1, Y_2)$ $sk \leftarrow (\alpha, x, y_1, y_2)$ Return (pk, sk)	$\widehat{\mathsf{XKG}}(\mathsf{pub} = (g,h), \mathsf{tag}^*)$: $z', z_1, z_2, z_3 \leftarrow \mathbb{Z}_p;\ X \leftarrow g^{z'} h^{-\mathsf{tag}^*}$ $Y_1 \leftarrow g^{z_1} h^{-z_2};\ Y_2 \leftarrow g^{z_3} Y_1^{-\mathsf{tag}^*}$ $pk \leftarrow (g, h, X, Y_1, Y_2)$ $\widehat{sk} \leftarrow (z', z_1, z_2, z_3, \mathsf{tag}^*)$ Return $(pk, \widehat{sk})$
$\mathsf{Pub}(pk, \mathsf{tag}, w)$: $\pi_1 \leftarrow (h^{\mathsf{tag}} X)^w; \pi_2 \leftarrow (Y_1^{\mathsf{tag}} Y_2)^w$ Return $\pi \leftarrow (\pi_1, \pi_2)$	$\widehat{\mathsf{Priv}}(\widehat{sk}, u)$: $\pi_1 \leftarrow u^{z'}; \pi_2 \leftarrow u^{z_3}$ Return $\pi \leftarrow (\pi_1, \pi_2)$
$\mathsf{Ext}(sk, \mathsf{tag}, u, \pi)$: If $u^{\alpha \cdot \mathsf{tag} + x} = \pi_1$ and $u^{y_1 \cdot \mathsf{tag} + y_2} = \pi_2$ then return $s \leftarrow u^{\alpha}$ else return $\perp$	$\widehat{\mathsf{Ext}}(\widehat{sk}, \mathsf{tag}, u, \pi)$: $s \leftarrow (\pi_1 \cdot u^{-z'})^{\frac{1}{\mathsf{tag} - \mathsf{tag}^*}}; s' \leftarrow (\pi_2 \cdot u^{-z_3})^{\frac{1}{\mathsf{tag} - \mathsf{tag}^*}}$ If $s^{z_2} s' = u^{z_1}$ then return s else return $\perp$

Fig. 3. The CS secure ABO-XHPS $\mathcal{X}_{\mathtt{CKS}}$. The internal hash function family is defined by $\mathsf{H}_{pk}(\mathsf{tag}, u) = ((h^{\mathsf{tag}} X)^w, (Y_1^{\mathsf{tag}} Y_2)^w)$ where $u = g^w$.

$K = \mathsf{G}(s)$ looks like a uniformly random value. This property is like *computational universal*$_2$ [17] for a "Cramer-Shoup" type HPS [7], and plays a key role for showing CCCA security of the ABO-XHPS-based KEMs that will be given in the next section. Formally, consider the experiment $\mathsf{Expt}^{\mathtt{PR\text{-}Ext}}_{\mathcal{X},\mathcal{A}}(k)$ that an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ runs in as in Fig. 2 (bottom-left). In the experiment, it is required that $(\mathsf{tag}', u', \pi')$ in $\mathcal{A}_2$'s output satisfy $\mathsf{tag}' \neq \mathsf{tag}^*$ and $\mathsf{H}_{pk}(\mathsf{tag}', u') \neq \pi'$.

Definition 4. *We say that an ABO-XHPS $\mathcal{X}$ has the* pseudorandom extraction *property* (PR-Ext *secure, for short), if the advantage* $\mathsf{Adv}^{\mathtt{PR\text{-}Ext}}_{\mathcal{X},\mathcal{A}}(k) = |\Pr[\mathsf{Expt}^{\mathtt{PR\text{-}Ext}}_{\mathcal{X},\mathcal{A}}(k) = 1] - 1/2|$ *is negligible for any PPTA $\mathcal{A}$.*

Concrete PR-Ext *Secure ABO-XHPS.* Here, we show a concrete ABO-XHPS based on the KEM by Hofheinz and Kiltz [17] and the KEM by Hanaoka and Kurosawa [13, Sect. 6], both of which are associated with the HDH-based Diffie-Hellman relation $\mathcal{R}^{\mathsf{DH}}$. The ABO-XHPS $\mathcal{X}_{\mathtt{HoKi}}$ based on [17] and the ABO-XHPS $\mathcal{X}_{\mathtt{HaKu}}$ based on [13, Sect. 6] are constructed as in Fig. 4. $\mathcal{X}_{\mathtt{HoKi}}$ can be proved PR-Ext secure roughly because the value z_2 generated in $\widehat{\mathsf{XKG}}$ is information-theoretically hidden from pk and values s extracted from a "correct" proof $\pi = \mathsf{H}_{pk}(\mathsf{tag}, u)$ using $\widehat{\mathsf{Ext}}$, while it appears in a value s extracted from an "invalid proof π satisfying $\pi \neq \mathsf{H}_{pk}(\mathsf{tag}, u)$ and makes the extracted value s look like a random value in $\mathbb{G}$. The value β generated in $\widehat{\mathsf{XKG}}$ of $\mathcal{X}_{\mathtt{HaKu}}$ plays a similar role. We also note that $\mathcal{X}_{\mathtt{HaKu}}$ satisfies only almost-correctness, as $\widehat{\mathsf{Ext}}$ cannot extract a value when $\mathsf{tag} = \beta$. However, it suffices for showing CCCA security of the ABO-XHPS-based KEM shown in the next section.

4.3 Weak Computational Soundness (wCS)

"*Weak computational soundness*" (wCS security) guarantees that it is hard to find an "invalid" proof $\pi \neq \mathsf{H}_{pk}(\mathsf{tag}, u)$ such that if we extract a value s with $\widehat{\mathsf{Ext}}$ from the invalid π, then the value s is the same as the value that is extracted from a "correct" proof

```
$\mathsf{XKG}(\mathsf{pub} = (g, h), \mathsf{pri} = \alpha)$ :
  $x_1, x_2 \leftarrow \mathbb{Z}_p$
  $X_i \leftarrow g^{x_i}$ for $i \in [2]$
  $pk \leftarrow (g, h, X_1, X_2)$
  $sk \leftarrow (\alpha, x_1, x_2)$
  Return $(pk, sk)$

$\widehat{\mathsf{XKG}}(\mathsf{pub} = (g, h), \mathsf{tag}^*)$ :
  $z_1, z_2, z_3 \leftarrow \mathbb{Z}_p$
  $X_1 \leftarrow g^{z_1} h^{z_2}$; $X_2 \leftarrow g^{z_3} h^{-z_2 \cdot \mathsf{tag}^*}$
  $pk \leftarrow (g, h, X_1, X_2)$
  $\widehat{sk} \leftarrow (z_1, z_2, z_3, \mathsf{tag}^*)$
  Return $(pk, \widehat{sk})$

$\mathsf{Pub}(pk, \mathsf{tag}, w)$ :
  $\pi \leftarrow (X_1^{\mathsf{tag}} X_2)^w$
  Return $\pi$

$\widehat{\mathsf{Priv}}(\widehat{sk}, u)$ :
  $\pi \leftarrow u^{z_1 \cdot \mathsf{tag}^* + z_3}$
  Return $\pi$

$\mathsf{Ext}(sk, \mathsf{tag}, u, \pi)$ :
  If $u^{x_1 \cdot \mathsf{tag} + x_2} = \pi$ then
    return $s \leftarrow u^{\alpha}$ else return $\bot$

$\widehat{\mathsf{Ext}}(\widehat{sk}, \mathsf{tag}, u, \pi)$ :
  $s \leftarrow (\pi \cdot u^{-(z_1 \cdot \mathsf{tag} + z_3)})^{\frac{1}{z_2(\mathsf{tag} - \mathsf{tag}^*)}}$
  Return $s$
```

```
$\mathsf{XKG}(\mathsf{pub} = (g, h), \mathsf{pri} = \alpha)$ :
  $a_0 \leftarrow \alpha$; $A_0 \leftarrow h$; $a_1, a_2 \leftarrow \mathbb{Z}_p$
  $A_i \leftarrow g^{x_i}$ for $i \in [2]$; Let $f(x) := \sum_{i=0}^{2} a_i x^i$
  $pk \leftarrow (g, A_0, A_1, A_2)$; $sk \leftarrow f(\cdot)$
  Return $(pk, sk)$

$\widehat{\mathsf{XKG}}(\mathsf{pub} = (g, h), \mathsf{tag}^*)$ :
  $\beta, z_1, z_2 \leftarrow \mathbb{Z}_p$; $A_0 \leftarrow h$
  Compute$^{(*)}$ $A_1 = g^{a_1}$ and $A_2 = g^{a_2}$ s.t.
        $(f(0), f(\mathsf{tag}^*), f(\beta)) = (\alpha, z_1, z_2)$
  $pk \leftarrow (g, A_0, A_1, A_2)$; $\widehat{sk} \leftarrow (\beta, z_1, z_2, \mathsf{tag}^*)$
  Return $(pk, \widehat{sk})$

$\mathsf{Pub}(pk, \mathsf{tag}, w)$ :
  Return $\pi \leftarrow (A_0 A_1^{\mathsf{tag}} A_2^{\mathsf{tag}^2})^w$

$\widehat{\mathsf{Priv}}(\widehat{sk}, u)$ :
  Return $\pi \leftarrow u^{z_1}$

$\mathsf{Ext}(sk, \mathsf{tag}, u, \pi)$ :
  If $u^{f(\mathsf{tag})} = \pi$ then
   return $s \leftarrow u^{\alpha}$ else return $\bot$

$\widehat{\mathsf{Ext}}(\widehat{sk}, \mathsf{tag}, u, \pi)$ :
  If $\mathsf{tag} = \beta$ then return $\bot$
  Let $f'$ be a degree-2 polynomial s.t.
    $(f'(\mathsf{tag}), f'(\mathsf{tag}^*), f'(\beta)) = (\log_u \pi, z_1, z_2)$
  Compute$^{(*)}$ and return $s \leftarrow u^{f'(0)}$
```

Fig. 4. The PR-Ext secure ABO-XHPS $\mathcal{X}_{\texttt{HoKi}}$ (left) and $\mathcal{X}_{\texttt{HaKu}}$ (right). The internal hash function family of $\mathcal{X}_{\texttt{HoKi}}$ is defined by $\mathsf{H}_{pk}(\mathsf{tag}, u) = (X_1^{\mathsf{tag}} X_2)^w$, and that of $\mathcal{X}_{\texttt{HaKu}}$ is defined by $\mathsf{H}_{pk}(\mathsf{tag}, u) = (A_0 A_1^{\mathsf{tag}} A_2^{\mathsf{tag}^2})^w$, where $u = g^w$. $^{(*)}$ In $\mathcal{X}_{\texttt{HaKu}}$, The values A_1 and A_2 in $\widehat{\mathsf{XKG}}$ and the value $u^{f'(0)}$ in $\widehat{\mathsf{Ext}}$ can be computed by Lagrange interpolation in the exponent [13].

$\pi' = \mathsf{H}_{pk}(\mathsf{tag}, u)$. Formally, consider the experiment $\mathsf{Expt}^{\texttt{wCS}}_{\mathcal{X},\mathcal{A}}(k)$ that an adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ runs in as in Fig. 2 (bottom-right).

Definition 5. *We say that an ABO-XHPS $\mathcal{X}$ satisfies* weak computational soundness (wCS *secure, for short), if the advantage* $\mathsf{Adv}^{\texttt{wCS}}_{\mathcal{X},\mathcal{A}}(k) = \Pr[\mathsf{Expt}^{\texttt{wCS}}_{\mathcal{X},\mathcal{A}}(k) = 1]$ *is negligible for any PPTA $\mathcal{A}$.*

We show that wCS security is indeed weaker than both CS and PR-Ext security.

Theorem 1. *Let $\mathcal{R}$ be a relation family and let $\mathcal{X}$ be an ABO-XHPS associated with $\mathcal{R}$. Assume that $\mathcal{R}$ is a one-way relation family, and $\mathcal{X}$ is either* CS *secure or* PR-Ext *secure. Then $\mathcal{X}$ is* wCS *secure.*

Intuition. If $\mathcal{X}$ is CS secure, then it is hard to find an invalid proof $\pi \neq \mathsf{H}_{pk}(\mathsf{tag}, u)$ from which we can extract some value that is not $\bot$, and thus wCS security is satisfied. If $\mathcal{X}$ is PR-Ext secure, then an extracted value s from an invalid proof $\pi \neq \mathsf{H}_{pk}(\mathsf{tag}, u)$ is pseudorandom, which will be different from the value $\widehat{\mathsf{Ext}}(\widehat{sk}, \mathsf{tag}, u, \mathsf{H}_{pk}(\mathsf{tag}, u))$ with overwhelming probability, and thus wCS security is satisfied.

Concrete wCS *Secure ABO-XHPS.* By definition, any ABO-XHPS whose $\widehat{\mathsf{Ext}}$ algorithm satisfies the "if-and-only-if"-style correctness of [27], is automatically wCS secure (and

$\mathsf{XKG}(\mathsf{pub} = (g, h), \mathsf{pri} = \alpha)$: $x \leftarrow \mathbb{Z}_p; X \leftarrow g^x$ Return $pk \leftarrow (g, h, X)$ and $sk \leftarrow (\alpha, x)$	$\widehat{\mathsf{XKG}}(\mathsf{pub} = (g, h), \mathsf{tag}^*)$: $z \leftarrow \mathbb{Z}_p; X \leftarrow g^z h^{-\mathsf{tag}^*}$ Return $pk \leftarrow (g, h, X)$ and $\widehat{sk} \leftarrow (z, \mathsf{tag}^*)$
$\mathsf{Pub}(pk, \mathsf{tag}, w)$: Return $\pi \leftarrow (h^{\mathsf{tag}} X)^w$	$\widehat{\mathsf{Priv}}(\widehat{sk}, u)$: Return $\pi \leftarrow u^z$
$\mathsf{Ext}(sk, \mathsf{tag}, u, \pi)$: If $u^{\alpha \cdot \mathsf{tag} + x} = \pi$ then return $s \leftarrow u^\alpha$ else return $\perp$	$\widehat{\mathsf{Ext}}(\widehat{sk}, \mathsf{tag}, u, \pi)$: Return $s \leftarrow (\pi \cdot u^{-z})^{\frac{1}{\mathsf{tag} - \mathsf{tag}^*}}$

Fig. 5. The wCS secure ABO-XHPS $\mathcal{X}_{\mathtt{Kiltz}}$. The internal hash function family is defined by $\mathsf{H}_{pk}(\mathsf{tag}, u) = (h^{\mathsf{tag}} X)^w$ where $u = g^w$.

hence all XHPS shown in [27] is wCS secure). Here, we show another concrete example of a wCS secure ABO-XHPS, which is based on the KEM by Kiltz [19] and is associated with the Diffie-Hellman relation family $\mathcal{R}^{\mathsf{DH}}$. (This is a variant of the (non-twin-)Diffie-Hellman-based ABO-XHPS in [27, Sect. 5.1].) Specifically, the example of the ABO-XHPS, which we call $\mathcal{X}_{\mathtt{Kiltz}}$, is as in Fig. 5. $\mathcal{X}_{\mathtt{Kiltz}}$ can be shown to be wCS secure because there is no tuple $(\mathsf{tag}, u, \pi, s)$ that satisfies the winning condition of an adversary $\mathcal{A}$ in the wCS experiment. Namely, if $\mathsf{tag} \neq \mathsf{tag}^*$ and $\pi \neq \mathsf{H}_{pk}(\mathsf{tag}, u)$, then it is guaranteed that $\widehat{\mathsf{Ext}}(\widehat{sk}, \mathsf{tag}, u, \pi) \neq \widehat{\mathsf{Ext}}(\widehat{sk}, \mathsf{tag}, u, \mathsf{H}_{pk}(\mathsf{tag}, u))$.

4.4 Combining PR-Ext and wCS to Obtain CS

Here, we propose a "transformation" for obtaining a CS secure ABO-XHPS from PR-Ext secure one and wCS secure one. Let $\mathcal{R}$ be a relation family, and for $i \in [2]$, let $\mathcal{X}_i = (\mathsf{XKG}_i, \mathsf{Pub}_i, \mathsf{Ext}_i, \widehat{\mathsf{XKG}}_i, \widehat{\mathsf{Priv}}_i, \widehat{\mathsf{Ext}}_i)$ be an ABO-XHPS which is associated with $\mathcal{R}$. Furthermore, let $\mathsf{H}^{(i)}$ be the internal hash function family of $\mathcal{X}_i$. Then, using $\mathcal{X}_1$ and $\mathcal{X}_2$ as building blocks, we construct another ABO-XHPS $\mathcal{X}' = (\mathsf{XKG}'$, Pub', Ext', $\widehat{\mathsf{XKG}}'$, $\widehat{\mathsf{Priv}}'$, $\widehat{\mathsf{Ext}}'$), which is associated with the same $\mathcal{R}$, as in Fig. 6. Let $PK = (pk_1, pk_2)$ be a public key of $\mathcal{X}'$. Then the internal hash function family H' of $\mathcal{X}'$ is defined by $\mathsf{H}'_{PK}(\mathsf{tag}, u) = (\pi_1, \pi_2) = (\mathsf{H}^{(1)}_{pk_1}(\mathsf{tag}, u), \mathsf{H}^{(2)}_{pk_2}(\mathsf{tag}, u))$.

The following theorem holds.

Theorem 2. *Let $\mathcal{R}$ be a relation family and let $\mathcal{X}_1$ and $\mathcal{X}_2$ be ABO-XHPS associated with $\mathcal{R}$. Assume that $\mathcal{R}$ is a one-way relation family, $\mathcal{X}_1$ and $\mathcal{X}_2$ are* PR-Ext *secure and* wCS *secure, respectively. Then the ABO-XHPS $\mathcal{X}'$ constructed as in Fig. 6 is* CS *secure.*

Intuition. In order for an adversary $\mathcal{A}$ against the CS security of $\mathcal{X}'$ to win, it has to make a query $(\mathsf{tag}, u, \pi = (\pi_1, \pi_2))$ of either of the following types: (1) $\mathsf{tag} \neq \mathsf{tag}^* \wedge \mathsf{H}^{(1)}_{pk_1}(\mathsf{tag}, u) \neq \pi_1 \wedge \widehat{\mathsf{Ext}}_1(\widehat{sk}_1, \mathsf{tag}, u, \pi_1) = \widehat{\mathsf{Ext}}_2(\widehat{sk}_2, \mathsf{tag}, u, \pi_2) \neq \perp$, or (2) $\mathsf{tag} \neq \mathsf{tag}^* \wedge \mathsf{H}^{(1)}_{pk_1}(\mathsf{tag}, u) = \pi_1 \wedge \mathsf{H}^{(2)}_{pk_2}(\mathsf{tag}, u) \neq \pi_2 \wedge \widehat{\mathsf{Ext}}_1(\widehat{sk}_1, \mathsf{tag}, u, \pi_1) = \widehat{\mathsf{Ext}}_2(\widehat{sk}_2, \mathsf{tag}, u, \pi_2) \neq \perp$. However, a tuple of the first type is hard to find due to the PR-Ext security of $\mathcal{X}_1$, because if the query is of first type, then the extracted value $s_1 = \widehat{\mathsf{Ext}}_1(\widehat{sk}_1, \mathsf{tag}, u, \pi_1)$ is a pseudorandom and is different from $s_2 = \widehat{\mathsf{Ext}}_2(\widehat{sk}_2, \mathsf{tag}, u, \pi_2)$

$\mathsf{XKG}'(\mathsf{pub},\mathsf{pri})$: $(pk_i, sk_i) \leftarrow \mathsf{XKG}_i(\mathsf{pub},\mathsf{pri})$ for $i \in [2]$ $PK \leftarrow (pk_1, pk_2)$; $SK \leftarrow (sk_1, sk_2)$ Return (PK, SK)	$\widehat{\mathsf{XKG}}'(\mathsf{pub},\mathsf{tag}^*)$: $(pk_i, \widehat{sk}_i) \leftarrow \widehat{\mathsf{XKG}}_i(\mathsf{pub},\mathsf{tag}^*)$ for $i \in [2]$ $PK \leftarrow (pk_1, pk_2)$; $\widehat{SK} \leftarrow (\widehat{sk}_1, \widehat{sk}_2)$ Return $(PK, \widehat{SK})$
$\mathsf{Pub}'(PK, \mathsf{tag}, w)$: $\pi_i \leftarrow \mathsf{Pub}_i(pk_i, \mathsf{tag}, w)$ for $i \in [2]$ Return $\pi \leftarrow (\pi_1, \pi_2)$	$\widehat{\mathsf{Priv}}'(\widehat{SK}, u)$: $\pi_i \leftarrow \widehat{\mathsf{Priv}}_i(\widehat{sk}_i, u)$ for $i \in [2]$ Return $\pi \leftarrow (\pi_1, \pi_2)$
$\mathsf{Ext}'(SK, \mathsf{tag}, u, \pi)$: $s_i \leftarrow \mathsf{Ext}_i(sk_i, \mathsf{tag}, u, \pi_i)$ for $i \in [2]$ If $s_1 = s_2 \neq \perp$ then return s_1 else return $\perp$	$\widehat{\mathsf{Ext}}'(\widehat{SK}, \mathsf{tag}, u, \pi)$: $s_i \leftarrow \widehat{\mathsf{Ext}}_i(\widehat{sk}_i, \mathsf{tag}, u, \pi_i)$ for $i \in [2]$ If $s_1 = s_2 \neq \perp$ then return s_1 else return $\perp$

Fig. 6. The transformation for obtaining a CS secure ABO-XHPS $\mathcal{X}'$ from a PR-Ext secure ABO-XHPS $\mathcal{X}_1$ and a wCS secure ABO-XHPS $\mathcal{X}_2$

with overwhelming probability, regardless of the value s_2. Furthermore, a query of the second type is also hard to find because such tuple can be directly used to break the wCS security of $\mathcal{X}_2$. More specifically, the condition $\mathsf{H}^{(1)}_{pk_1}(\mathsf{tag}, u) = \pi_1$ guarantees $s_1 = \widehat{\mathsf{Ext}}_1(\widehat{sk}_1, \mathsf{tag}, u, \pi_1) = \widehat{\mathsf{Ext}}_2(\widehat{sk}_2, \mathsf{tag}, u, \mathsf{H}^{(2)}_{pk_2}(\mathsf{tag}, u))$ due to the correctness of the all-but-one mode of ABO-XHPS. Therefore, the tuple $(\mathsf{tag}, u, \pi_2, s_1)$ with $\mathsf{tag} \neq \mathsf{tag}^*$ and $\mathsf{H}^{(2)}_{pk_2}(\mathsf{tag}, u) \neq \pi_2$ satisfies the winning condition of the wCS experiment.

5 KEMs Based on ABO-XHPS

In this section, we show our results regarding the KEMs based on ABO-XHPS. Specifically, we show that CCA security of the ABO-XHPS-based KEM can be shown without using gap version of one-way relation families and the stronger correctness requirement defined in [27], and instead a (non-gap) one-way relation family and our weaker correctness, together with CS security, suffices. Furthermore, we show that the KEM can be shown to be CCCA secure if the ABO-XHPS satisfies PR-Ext security. Finally, we show that using the ABO-XHPS in a slightly different way, the ABO-XHPS-based KEM can be extended to be a (C)CCA secure MR-KEM.

5.1 Single-Recipient KEM

Let $\mathcal{R} = (\mathsf{RSetup}, \mathsf{RSamp}, \mathsf{G})$ be a relation family, $\mathcal{X} = (\mathsf{XKG}, \mathsf{Pub}, \mathsf{Ext}, \widehat{\mathsf{XKG}}, \widehat{\mathsf{Priv}}, \widehat{\mathsf{Ext}})$ be an ABO-XHPS associated with $\mathcal{R}$, and $\mathsf{TCR} : \mathcal{U} \rightarrow \mathcal{T}$ be a target collision resistant hash function (TCRHF).[3] Then we construct a KEM $\Gamma_1 = (\mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ based on the ABO-XHPS $\mathcal{X}$ as in Fig. 7 (left).

[3] Roughly, an efficiently computable function TCR is said to be a TCRHF if given a random input x, it is hard to find another input x' such that $\mathsf{TCR}(x) = \mathsf{TCR}(x') \wedge x \neq x'$. The formal definition can be found in the full version or in the papers [19,17,12,18,27].

```
$\mathsf{KG}(1^k)$ :
  $(\mathsf{pub}, \mathsf{pri}) \leftarrow \mathsf{RSetup}(1^k)$
  $(pk, sk) \leftarrow \mathsf{XKG}(\mathsf{pub}, \mathsf{pri})$
  Return $(pk, sk)$

$\mathsf{Enc}(pk)$ :
  $w \leftarrow \mathcal{W}$
  $(u, s) \leftarrow \mathsf{RSamp}(w)$
  $\mathsf{tag} \leftarrow \mathsf{TCR}(u)$
  $\pi \leftarrow \mathsf{Pub}(pk, \mathsf{tag}, w)$
  $c \leftarrow (u, \pi)$; $K \leftarrow \mathsf{G}(s)$
  Return $(c, K)$

$\mathsf{Dec}(sk, c)$ :
  $(u, \pi) \leftarrow c$; $\mathsf{tag} \leftarrow \mathsf{TCR}(u)$
  $s \leftarrow \mathsf{Ext}(sk, \mathsf{tag}, u, \pi)$
  If $s = \perp$ then return $\perp$
  Return $K \leftarrow \mathsf{G}(s)$
```

```
$\mathsf{MSetup}(1^k)$ :
  $(\mathsf{pub}, \mathsf{pri}) \leftarrow \mathsf{RSetup}(1^k)$
  Return $\mathsf{pub}$

$\mathsf{MKG}(\mathsf{pub})$ :
  $\mathsf{dummy} \leftarrow \mathcal{T}$
  $(pk, \widehat{sk}) \leftarrow \widehat{\mathsf{XKG}}(\mathsf{pub}, \mathsf{dummy})$
  $SK \leftarrow (\widehat{sk}, \mathsf{dummy})$
  Return $(pk, SK)$

$\mathsf{MExt}(pk_i, c)$ :
  $(u, \boldsymbol{\pi}) \leftarrow c$; $(\pi_1, \dots, \pi_n) \leftarrow \boldsymbol{\pi}$
  Return $c_i \leftarrow (u, \pi_i)$

$\mathsf{MEnc}(\mathbf{pk})$ :
  $(pk_1, \dots, pk_n) \leftarrow \mathbf{pk}$
  $w \leftarrow \mathcal{W}$
  $(u, s) \leftarrow \mathsf{RSamp}(w)$
  $\mathsf{tag} \leftarrow \mathsf{TCR}(u)$
  $\pi_i \leftarrow \mathsf{Pub}(pk_i, \mathsf{tag}, w)$
                                   for $i \in [n]$
  $\boldsymbol{\pi} \leftarrow (\pi_1, \dots, \pi_n)$
  $c \leftarrow (u, \boldsymbol{\pi})$; $K \leftarrow \mathsf{G}(s)$
  Return $(c, K)$

$\mathsf{MDec}(SK_i, c_i)$ :
  $(\widehat{sk}_i, \mathsf{dummy}_i) \leftarrow SK_i$; $(u, \pi_i) \leftarrow c_i$; $\mathsf{tag} \leftarrow \mathsf{TCR}(u)$
  If $\mathsf{tag} \neq \mathsf{dummy}_i$ and $s = \widehat{\mathsf{Ext}}(\widehat{sk}_i, \mathsf{tag}, u, \pi_i) \neq \perp$
                                   then return $K \leftarrow \mathsf{G}(s)$ else return $\perp$
```

Fig. 7. The (single-recipient) KEM Γ_1 (left) and the MR-KEM Γ_M (right)

CCA Security. Wee [27] showed the following.[4]

Theorem 3. *([27]) If $\mathcal{R}$ is a gap one-way relation family, $\mathcal{X}^{\mathcal{R}}$ is an ABO-XHPS, and* TCR *is a TCRHF, then the KEM Γ_1 is* CCA *secure.*

We show that the same KEM Γ_1 can be proved in the following way, without using a "gap" one-way relation family.

Theorem 4. *If $\mathcal{R}$ is a one-way relation family, $\mathcal{X}^{\mathcal{R}}$ is an ABO-XHPS which satisfies* CS *security, and* TCR *is a TCRHF, then the KEM Γ_1 is* CCA *secure.*

Intuition. To ensure that the real challenge key $K_1^* = \mathsf{G}(s^*)$ looks random for a CCA adversary $\mathcal{A}$, we have to use pseudorandomness of the generator G of the one-way relation $\mathcal{R}$. However, the reduction algorithm $\mathcal{B}$, who attacks pseudorandomness of G, needs to simulate the CCA experiment for $\mathcal{A}$ without knowing the private parameter pri or the randomness w^* used to sample $(u^*, s^*) \in \mathcal{R}_{\mathsf{pub}}$. $\mathcal{B}$ therefore simulates the CCA experiment for $\mathcal{A}$ by using the all-but-one mode of the ABO-XHPS $\mathcal{X}$. The $\widehat{\mathsf{Priv}}$ algorithm enables $\mathcal{B}$ to generate the challenge ciphertext $c^* = (u^*, \pi^*)$ correctly, using $\widehat{sk}$ output from $\widehat{\mathsf{XKG}}(\mathsf{pub}, \mathsf{tag}^*)$ where $\mathsf{tag}^* = \mathsf{TCR}(u^*)$. However, since we do not use "gap" one-way relation family, $\mathcal{B}$ does not have access to the relation oracle $\mathcal{R}_{\mathsf{pub}}$, and thus cannot check inconsistency of a ciphertext by itself. Here, CS security of $\mathcal{X}$ guarantees that even if $\mathcal{A}$ submits an invalid ciphertext $c = (u, \pi)$ with $\mathsf{H}_{pk}(\mathsf{TCR}(u), u) \neq \pi$, the $\widehat{\mathsf{Ext}}$ algorithm almost perfectly works like the Ext algorithm in the real decapsulation algorithm in Dec of Γ_1. In doing so, the TCRHF TCR enables $\mathcal{B}$ to always use $\widehat{\mathsf{Ext}}$,

[4] As we have mentioned, Wee's definition of ABO-XHPS in [27] requires stronger correctness for $\widehat{\mathsf{Ext}}$ algorithm. However, CCA security of the ABO-XHPS-based KEM can be shown without this requirement.

so that the problematic situation where $\mathsf{tag} = \mathsf{TCR}(u) = \mathsf{tag}^*$ never occurs. Then, indistinguishability of two modes guarantees that $\mathcal{A}$'s behavior cannot be non-negligibly different between the case in which the experiment is simulated by $\mathcal{B}$ with the all-but-one mode, and the case in which $\mathcal{A}$ is in the original CCA experiment.

CCCA Security. We show that the KEM Γ_1 based on the ABO-XHPS $\mathcal{X}$ is CCCA secure, when $\mathcal{X}$ is PR-Ext secure.

Theorem 5. *If $\mathcal{R}$ is a one-way relation family, $\mathcal{X}^{\mathcal{R}}$ is an ABO-XHPS which satisfies* PR-Ext *security, and* TCR *is a TCRHF, then the KEM Γ_1 is* CCCA *secure.*

Intuition. The intuitive explanation on the proof of this theorem is very close to that of Theorem 4. The difference is that we can no longer expect that the $\widehat{\mathsf{Ext}}$ algorithm can be used to reject an invalid ciphertext $c = (u, \pi)$ with $\pi \neq \mathsf{H}_{pk}(\mathsf{TCR}(u), u)$, because $\mathcal{X}$ is not guaranteed to be CS secure. However, recall that PR-Ext security of $\mathcal{X}$ guarantees that an extracted value s from an invalid input is a pseudorandom value in $\mathcal{S}$, which in turn guarantees that $K = \mathsf{G}(s) \in \mathcal{K}$ is also pseudorandom and thus unpredictable to the adversary $\mathcal{A}$. Recall also that a valid CCCA adversary has to control its "uncertainty" to be negligible. These help that $\mathcal{A}$'s CDEC query with an invalid ciphertext is "implicitly" rejected, and thus the main reduction algorithm $\mathcal{B}$'s simulation of the CCCA experiment for $\mathcal{A}$ are guaranteed to be almost perfect.

5.2 Multi-Recipient KEM

Here, we show how to construct a MR-KEM using ABO-XHPS. Using the same building blocks ($\mathcal{R}$, $\mathcal{X}$, and TCR) as in Γ_1, we construct a MR-KEM $\Gamma_M = (\mathsf{MSetup}, \mathsf{MKG}, \mathsf{MEnc}, \mathsf{MExt}, \mathsf{MDec})$ as in Fig. 7 (right).

The main feature of the MR-KEM Γ_M is that we use the all-but-one mode of the underlying ABO-XHPS $\mathcal{X}$ even for normal operations, namely, each user's key is setup with $\widehat{\mathsf{XKG}}$ using a "dummy tag" dummy. This is to setup users' keys without using the private parameter pri corresponding to pub, which makes it possible to share pub with many users. Since $\widehat{\mathsf{Ext}}$ cannot extract a value when it is invoked with the tag that is used to generate $\widehat{sk}$, the decapsulation algorithm MDec rejects a user i's ciphertext $c = (u, \pi_i)$ satisfying $\mathsf{TCR}(u) = \mathsf{dummy}$, even if c is honestly generated by using MEnc. Therefore, our MR-KEM Γ_M does not have perfect correctness. However, it satisfies *almost-correctness*: The information on dummy in a user's secret key is information-theoretically hidden from entities other than the user who holds dummy. Therefore, it is hard to find a ciphertext $c = (u, \boldsymbol{\pi})$ that satisfies $\mathsf{TCR}(u) = \mathsf{dummy}$, regardless of the validity of c.

Hiwatari et al. [16] proposed two MR-KEMs. Their first scheme, which is CCA secure, is based on the KEM by [6, Sect. 5.2], while their second scheme, which is CCCA secure, is based on the KEM by [13, Sect. 5]. Both of their schemes can be seen as concrete instantiations of the MR-KEM Γ_M: Their first one is based on the ABO-XHPS $\mathcal{X}_{\mathtt{CKS}}$, while their second one is based on the ABO-XHPS $\mathcal{X}_{\mathtt{HaKu}}$. From another viewpoint, our MR-KEM based on ABO-XHPS is a generalization of Hiwatari et al.

Theorem 6. *If $\mathcal{R}$ is a one-way relation, $\mathcal{X}^{\mathcal{R}}$ is an ABO-XHPS which satisfies* CS *security, and* TCR *is a TCRHF, then the MR-KEM Γ_M is* CCA *secure.*

Theorem 7. *If $\mathcal{R}$ is a one-way relation, $\mathcal{X}^{\mathcal{R}}$ is an ABO-XHPS which satisfies* $\mathtt{PR\text{-}Ext}$ *security, and* TCR *is a TCRHF, then the MR-KEM Γ_M is* $\mathtt{CCCA}$ *secure.*

The proofs proceed similarly to those of Theorems 4 and 5. The difference is that here, we start from the situation in which each user's key is generated by $\widehat{\mathsf{XKG}}$ with dummy tag dummy, while in the proofs of Theorems 4 and 5, we started from the situation in which each user's key is generated by XKG. We also have to deal with the difference between multi-recipient (n users) and single-recipient environments, but this can be essentially dealt with users' key-wise hybrid argument.

6 Discussion

Capturing a Wider Class of Constructions and Security Proofs. We see that by our results, the framework of KEMs based on ABO-XHPS captures most practical $\mathtt{(C)CCA}$ secure KEMs. Concretely, many existing $\mathtt{CCA}$ secure KEMs can be seen as concrete instantiations derived from our extended framework, which include KEMs by Boyen et al. [5], Cash et al. [6, Sect. 5.2], and Hanaoka and Kurosawa [13, Sect. 4], and the $\mathtt{CCCA}$ secure KEMs by Hofheinz and Kiltz [17] and Hanaoka and Kurosawa [13, Sect. 6].

Interestingly, the extraction mode of the ABO-XHPS $\mathcal{X}_{\mathtt{CKS}}$ based on the Cash et al. KEM [6, Sect. 5.2] is exactly the same as that of the $\mathtt{CS}$ secure ABO-XHPS obtained via the transformation (Theorem 2) using the $\mathtt{PR\text{-}Ext}$ secure ABO-XHPS $\mathcal{X}_{\mathtt{HoKi}}$ and the $\mathtt{wCS}$ secure ABO-XHPS $\mathcal{X}_{\mathtt{Kiltz}}$. Therefore, Theorems 2 and 4 provide us with an alternative proof of $\mathtt{CCA}$ security of Cash et al. KEM, without using the trapdoor test theorem [6, Theorem 2]. We see that this is a concrete evidence that our results are useful for understanding constructions and security proofs of practical $\mathtt{CCA}$ secure KEMs in a modular manner.

As is the same with the original framework [27], our results also work for k-wise product relation (i.e. k-independent copies of relation families). This extension is useful to capture hardcore bit-based constructions of KEMs in the framework of ABO-XHPS. However, the clear disadvantage of this approach is that the ciphertext size of the KEM derived from the ABO-XHPS for the k-wise product relation becomes linear in k.

Strictly speaking, ours (and the original framework in [27]) still does not capture the $\mathtt{CCA}$ secure KEMs whose session-key is derived using hardcore bits but whose ciphertext size is constant (e.g. [13,14,15,29]). Technically, the security proofs of these KEMs require hybrid argument to replace the real session-key bit-by-bit to finally reach the game in which the real session-key is truly random (and thus an adversary has zero advantage), while the security proofs of the ABO-XHPS-based KEMs in our work and in [27], do not allow this approach. Moreover, it seems to us that how to derive many hardcore-bits in each scheme is quite dependent on the algebraic structure of the constructions. However, we note that at least the "basic structures" of the KEMs in [15,29], which do not consider hardcore-bit-based session-key derivation but derive key by considering "the corresponding (hashed version of) decisional problems, can be seen as concrete instantiations from our extended framework. To extend the framework of ABO-XHPS-based KEMs further to capture these constructions will be worth tackling.

New Instantiations of (MR-)KEMs. Due to Theorems 4, 5, 6, and 7, we can derive a number of new $(\mathtt{C})\mathtt{CCA}$ secure (MR-)KEMs. Specifically, due to Theorem 2, we can construct a $\mathtt{CS}$ secure ABO-XHPS from a $\mathtt{PR\text{-}Ext}$ secure ABO-XHPS and a $\mathtt{wCS}$ secure ABO-XHPS, or from two $\mathtt{PR\text{-}Ext}$ secure ABO-XHPS via Theorem 1 (i.e. one of the two ABO-XHPS is treated as a $\mathtt{wCS}$ secure ABO-XHPS). Therefore, using the ABO-XHPS we show in Section 4, we can derive a number of variants of KEMs [8,6,12]: we can obtain a $\mathtt{CS}$ secure ABO-XHPS by the combination of $\mathcal{X}_{\mathtt{HoKi}}$ and $\mathcal{X}_{\mathtt{Kiltz}}$ (which happens to be essentially identical to $\mathcal{X}_{\mathtt{CKS}}$ as mentioned above) and the combination of $\mathcal{X}_{\mathtt{HaKu}}$ and $\mathcal{X}_{\mathtt{Kiltz}}$. We can also obtain a new $\mathtt{CS}$ ABO-XHPS by combining $\mathcal{X}_{\mathtt{HoKi}}$ and $\mathcal{X}_{\mathtt{HaKu}}$, two independent instances of $\mathcal{X}_{\mathtt{HoKi}}$, and two independent instances of $\mathcal{X}_{\mathtt{HaKu}}$. Then, from these $\mathtt{CS}$ secure ABO-XHPS, we derive new $\mathtt{CCA}$ secure KEMs and MR-KEMs, due to Theorems 4 and 6, respectively.

Furthermore, we can also obtain a number of practical MR-KEMs from existing ABO-XHPS. For example, from the $\mathtt{CS}$ secure ABO-XHPS based on the KEM by Boyen et al. [5] (which can be found the full version), we obtain a $\mathtt{CCA}$ secure MR-KEM based on the DBDH assumption whose ciphertext size is $n + 1$ group elements when sending to n recipients. This construction is the most efficient $\mathtt{CCA}$ secure MR-KEM in terms of ciphertext size. Moreover, by using the factoring-based ABO-XHPS shown in [27, Sect. 4.2] (which is $\mathtt{CS}$ secure), we obtain a $\mathtt{CCA}$ secure factoring-based MR-KEM which is more efficient than the construction that naively concatenates the ciphertexts from a single-recipient KEM by Hofheinz and Kiltz [18].

Finally, we stress that the advantages of our results are not only the efficiency of the concretely derived (MR-)KEMs, but also the strengthening of the framework of [27], which we believe is useful for future design of $(\mathtt{C})\mathtt{CCA}$ secure (MR-)KEMs.

Acknowledgement. The authors would like to thank anonymous reviewers and the members of Shin-Akarui-Angou-Benkyou-Kai for their invaluable comments and suggestions. The first author is supported by the JSPS Fellowships for Young Scientists.

References

1. Bellare, M., Boldyreva, A., Kurosawa, K., Staddon, J.: Multirecipient encryption schemes: How to save on bandwidth and computation without sacrificing security. IEEE Trans. Inf. Theory 53(11), 3927–3943 (2007)
2. Bellare, M., Namprempre, C.: Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 531–545. Springer, Heidelberg (2000)
3. Boneh, D., Canetti, R., Halevi, S., Katz, J.: Chosen-ciphertext security from identity-based encryption. SIAM J. Comput. 36(5), 1301–1328 (2007)
4. Boyen, X., Mei, Q., Waters, B.: Direct chosen ciphertext security from identity-based techniques. In: ACMCCS 2005, pp. 320–329 (2005)
5. Boyen, X., Mei, Q., Waters, B.: Direct chosen ciphertext security from identity-based techniques. Updated version of [4]. Cryptology ePrint Archive: Report 2005/288 (2005), `http://eprint.iacr.org/2005/288/`

6. Cash, D., Kiltz, E., Shoup, V.: The Twin Diffie-Hellman Problem and Applications. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 127–145. Springer, Heidelberg (2008)
7. Cramer, R., Shoup, V.: Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 45–64. Springer, Heidelberg (2002)
8. Cramer, R., Shoup, V.: Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM J. Comput. 33(1), 167–226 (2003)
9. Dolev, D., Dwork, C., Naor, M.: Non-malleable cryptography. In: STOC 1991, pp. 542–552 (1991)
10. Elkind, E., Sahai, A.: A unified methodology for constructing public-key encryption schemes secure against adaptive chosen-ciphertext attack. Cryptology ePrint Archive: Report 2002/042 (2002), http://eprint.iacr.org/2002/042/
11. Gennaro, R., Krawczyk, H., Rabin, T.: Secure Hashed Diffie-Hellman over Non-DDH Groups. In: Cachin, C., Camenisch, J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 361–381. Springer, Heidelberg (2004)
12. Hanaoka, G., Kurosawa, K.: Efficient Chosen Ciphertext Secure Public Key Encryption under the Computational Diffie-Hellman Assumption. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 308–325. Springer, Heidelberg (2008)
13. Hanaoka, G., Kurosawa, K.: Efficient chosen ciphertext secure public key encryption under the computational Diffie-Hellman assumption. Full version of [12]. Cryptology ePrint Archive: Report 2008/211 (2008), http://eprint.iacr.org/2008/211/
14. Hanaoka, G., Kurosawa, K.: Between hashed DH and computational DH: Compact encryption from weaker assumption. IEICE Transactions E93-A(11), 1994–2006 (2010)
15. Haralambiev, K., Jager, T., Kiltz, E., Shoup, V.: Simple and Efficient Public-Key Encryption from Computational Diffie-Hellman in the Standard Model. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 1–18. Springer, Heidelberg (2010)
16. Hiwatari, H., Tanaka, K., Asano, T., Sakumoto, K.: Multi-recipient Public-Key Encryption from Simulators in Security Proofs. In: Boyd, C., González Nieto, J. (eds.) ACISP 2009. LNCS, vol. 5594, pp. 293–308. Springer, Heidelberg (2009)
17. Hofheinz, D., Kiltz, E.: Secure Hybrid Encryption from Weakened Key Encapsulation. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 553–571. Springer, Heidelberg (2007)
18. Hofheinz, D., Kiltz, E.: Practical Chosen Ciphertext Secure Encryption from Factoring. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 313–332. Springer, Heidelberg (2009)
19. Kiltz, E.: Chosen-Ciphertext Secure Key-Encapsulation Based on Gap Hashed Diffie-Hellman. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 282–297. Springer, Heidelberg (2007)
20. Kurosawa, K., Desmedt, Y.: A New Paradigm of Hybrid Encryption Scheme. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 426–442. Springer, Heidelberg (2004)
21. Naor, M., Yung, M.: Universal one-way hash functions and their cryptographic applications. In: STOC 1989, pp. 33–43 (1989)
22. Naor, M., Yung, M.: Public-key cryptosystems provably secure against chosen ciphertext attacks. In: STOC 1990, pp. 427–437 (1990)
23. Peikert, C., Waters, B.: Lossy trapdoor functions and their applications. In: STOC 2008, pp. 187–196 (2008)
24. Rackoff, C., Simon, D.R.: Non-interactive Zero-Knowledge Proof of Knowledge and Chosen Ciphertext Attack. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 433–444. Springer, Heidelberg (1992)

25. Sahai, A.: Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security. In: FOCS 1999, pp. 543–553 (1999)
26. Smart, N.P.: Efficient Key Encapsulation to Multiple Parties. In: Blundo, C., Cimato, S. (eds.) SCN 2004. LNCS, vol. 3352, pp. 208–219. Springer, Heidelberg (2005)
27. Wee, H.: Efficient Chosen-Ciphertext Security via Extractable Hash Proofs. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 314–332. Springer, Heidelberg (2010)
28. Wee, H.: Threshold and Revocation Cryptosystems via Extractable Hash Proofs. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 589–609. Springer, Heidelberg (2011)
29. Yamada, S., Kawai, Y., Hanaoka, G., Kunihiro, N.: Public key encryption schemes from the (B)CDH assumption with better efficiency. IEICE Transactions 93-A(11), 1984–1993 (2010)