Tight Leakage-Resilient CCA-Security from Quasi-Adaptive Hash Proof System*

Shuai Han[1,4], Shengli Liu[1,2,3(✉)], Lin Lyu[1], and Dawu Gu[1]

[1] School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
{dalen17,slliu,lvlin,dwgu}@sjtu.edu.cn
[2] State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China
[3] Westone Cryptologic Research Center, Beijing 100070, China
[4] Ant Financial, Hangzhou 310012, China

Abstract. We propose the concept of quasi-adaptive hash proof system (QAHPS), where the projection key is allowed to depend on the specific language for which hash values are computed. We formalize leakage-resilient(LR)-ardency for QAHPS by defining two statistical properties, including LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-universal and LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-key-switching.

We provide a generic approach to tightly leakage-resilient CCA (LR-CCA) secure public-key encryption (PKE) from LR-ardent QAHPS. Our approach is reminiscent of the seminal work of Cramer and Shoup (Eurocrypt'02), and employ three QAHPS schemes, one for generating a uniform string to hide the plaintext, and the other two for proving the well-formedness of the ciphertext. The LR-ardency of QAHPS makes possible the tight LR-CCA security. We give instantiations based on the standard k-Linear (k-LIN) assumptions over asymmetric and symmetric pairing groups, respectively, and obtain fully compact PKE with tight LR-CCA security. The security loss is $O(\log Q_e)$ where Q_e denotes the number of encryption queries. Specifically, our tightly LR-CCA secure PKE instantiation from SXDH has only 4 group elements in the public key and 7 group elements in the ciphertext, thus is the most efficient one.

1 Introduction

Tightly Secure Public-Key Encryption. Usually, the security proof of a public-key encryption (PKE) scheme is accomplished through a security reduction. In a security reduction, any probabilistic polynomial-time (PPT) adversary $\mathcal{A}$ successfully attacking the PKE scheme with advantage $\epsilon_{\mathcal{A}}$ is converted to another PPT algorithm $\mathcal{B}$ that solves a specific problem with advantage $\epsilon_{\mathcal{B}}$, such that $\epsilon_{\mathcal{A}} \leq \ell \cdot \epsilon_{\mathcal{B}}$. Here ℓ is called the security loss factor. If ℓ is a polynomial in the number of encryption queries Q_e and/or the number of decryption queries Q_d, the security reduction is called a loose one. To achieve a target security level, one has to augment the security parameter λ to compensate for the security loss ℓ. If Q_e (Q_d) is large, say 2^{30}, a loose reduction will pay the price of inefficiency, since the compensation will slow the algorithms of PKE and enlarge the sizes of public/secret key and ciphertexts. Therefore, it is desirable that ℓ is a constant or only linear in the security parameter λ. Such a security reduction is called a tight one or an almost tight one.

Starting from the work of Bellare et al. [BBM00], brilliant works have been done in the construction of tightly (multi-challenge) IND-CCA secure PKE. Hofheinz and Jager [HJ12] designed the first tightly IND-CCA secure PKE from a standard assumption. More efficient constructions follow in [CW13, LPJY14, LPJY15, AHY15, GCD+16, Hof16, GHKW16, Hof17, GHK17].

Leakage-Resilient Security. The traditional security requirements for PKE are indistinguishability under chosen-plaintext attacks (IND-CPA) and chosen-ciphertext attacks (IND-CCA), which implicitly assume that the secret key of PKE is completely hidden from adversaries. In practice, however, various kinds of side-channel attacks on the physical implementation of the PKE algorithms [HSH+08] demonstrated that partial information about the secret key might be leaked to the attackers, thus threaten the security of PKE. To deal with key leakage, Akavia et al. [AGV09] and Naor and Segev

* A preliminary version of this paper was accepted by CRYPTO 2019 and this is the full version.

[NS09] formalized the leakage-resilient (LR) security model and defined LR-CPA/CCA securities, which stipulate the PKE remain IND-CPA/CCA secure even if an adversary has access to a leakage oracle and obtains additional information about the secret key. In this work, we focus on the bounded leakage-resilient model [AGV09], where the total amount of key leakage is bounded.

Generally, there are two approaches for designing PKE with LR-CCA security. The first is an adaption of the Naor-Yung double encryption paradigm [NY90] to the LR setting. Through this approach, an LR-CPA secure PKE can be upgraded to an LR-CCA secure one, with the help of a simulation-sound non-interactive zero-knowledge proof system (SS-NIZK) [NS09, KW15] or a true-simulation extractable NIZK (tSE-NIZK) [DHLAW10]. However, the resulting PKE may not be efficient due to the usage of SS-NIZK/tSE-NIZK. The second approach utilizes the more efficient Cramer-Shoup hash proof system (HPS) paradigm [CS02] based on the fact that HPS is intrinsically leakage-resilient [NS09]. Through this approach, many efficient LR-CCA secure PKE schemes were designed [QL13, FV16, FX16].

Efficient PKE with Tight LR-CCA Security. Although great progress was made on tight IND-CCA security, only Abe et al. [ADK+13] ever considered LR-CCA secure PKE with a tight security reduction. They followed the Naor-Yung paradigm and employed a tightly secure tSE-NIZK. Due to the tightness-preserving of the Naor-Yung paradigm, the resulting PKE is tightly LR-CCA secure. However, their PKE is highly impractical. The ciphertext of their PKE contains more than 800 group elements. Even plugging in the recent efficient and tightly secure SS-NIZKs/tSE-NIZKs [GHKW16, GHKP18][1], the resulting LR-CCA secure PKE still contains over 100 group elements in the public key or around 40 group elements in the ciphertext, thus is far from practical. A most recent work by Abe et al. [AJOR18a] presented a construction of QA-NIZK with tight unbounded simulation-soundness (USS) based on the MDDH assumptions and tried to use it to obtain a tightly CCA-secure PKE via the paradigm of CPA-PKE + USS-QA-NIZK. It is also possible to achieve tight LR-CCA security if the underlying PKE building block is LR-CPA secure. Unfortunately, their USS-QA-NIZK suffers from an attack, as shown in their full-version paper [AJOR18b] (in which the QA-NIZK was updated to a new one but its USS security remains to be justified).

For the sake of efficiency, one might like to try the second approach to LR-CCA security. However, the Cramer-Shoup HPS paradigm [CS02, NS09] does not work well in the face of multi-challenge ciphertexts (cf. Subsect. 1.1 for a detailed explanation). To pursue tight security reduction, great effort has been devoted to new designs of PKE from variants of HPS [GHKW16, GHK17]. Gay et al. [GHKW16] used combinations of multiple HPSs to construct PKE and proved its tight IND-CCA security (not LR-CCA), but at the price of more than 100 group elements in the public key. Gay et al. [GHK17] evolved HPS to a so-called "qualified proof system" (QPS) to obtain tightly IND-CCA secure PKE with full compactness (compact ciphertext and compact public key). However, their PKE is unlikely to be LR-CCA secure.[2] Up to now, there is no available approach to efficient PKE with tight LR-CCA security.

Our Contribution. In this paper, we propose a novel approach to the design of tightly LR-CCA secure PKE. More precisely,

- We propose the concept of quasi-adaptive HPS (QAHPS), and formalize LR-ardency for QAHPS by defining two statistical properties, including LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-universal and LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-key-switching. Our LR-ardent QAHPS generalizes the well-known universal$_1$, universal$_2$ [CS02] and extracting [DKPW12] HPSs.

[1] Gay et al. [GHKP18] constructed the state-of-the-art tightly secure (structure-preserving) signature schemes, where the signature is comprised of 14 group elements. By applying the framework in [HJ12, ADK+13], this signature scheme can be transformed to a tightly secure SS-NIZK/tSE-NIZK whose proof contains around 40 group elements.

[2] The properties of "constrained soundness" and "extensibility" of QPS are needed for the tight IND-CCA security proof of the PKE proposed by Gay et al. [GHK17]. We note that these two properties of their QPS are unlikely to hold when partial information about the secret key of QPS is leaked to adversary. See Appendix B for more details. Thus it is reasonable to conjecture that their PKE is not LR-CCA secure.

Table 1. Comparison among tightly (LR-)CCA secure PKE schemes. Here λ denotes the security parameter and $Q_e = \mathsf{poly}(\lambda)$ the number of challenge ciphertexts. $|PK|$ and $|C| - |M|$ show the size of public key and ciphertext overhead, where size means the number of group elements in the underlying groups. "k-LIN" is short for the k-Linear assumption. For pairing-free groups, 1-LIN = DDH; for asymmetric pairing groups, 1-LIN = SXDH, which requires the DDH assumption hold in both $\mathbb{G}_1$ and $\mathbb{G}_2$. "sym" stands for symmetric pairing groups and "asym" asymmetric pairing groups. "LR?" asks whether the security is proved in the leakage-resilient setting. We note that the security loss $O(\log Q_e)= O(\log \lambda)$ is lower than $O(\lambda)$.

Scheme	$\|PK\|$	$\|C\| - \|M\|$	Sec. loss	Assumption	Pairing	LR?
LPJY15 [LPJY14, LPJY15]	$O(\lambda)$	47	$O(\lambda)$	2-LIN	yes (sym)	—
AHY15 [AHY15]	$O(\lambda)$	12	$O(\lambda)$	2-LIN	yes (sym)	—
GCDCT16 [GCD+16]	$O(\lambda)$	$6k$	$O(\lambda)$	k-LIN ($k \geq 1$)	yes (asym)	—
GHKW16 [GHKW16]	$O(\lambda)$	$3k$	$O(\lambda)$	k-LIN ($k \geq 1$)	no	—
Hof16 [Hof16]	2	60	$O(\lambda)$	1-LIN = SXDH	yes (asym)	—
Hof17 [Hof17]	28 (resp. $2k^2 + 10k$)	6 (resp. $k + 4$)	$O(\lambda)$	2-LIN (resp. k-LIN)	yes (sym)	—
Hof17 [Hof17]	20	28	$O(\lambda)$	DCR	—	—
GHK17 [GHK17]	6	3	$O(\lambda)$	1-LIN = DDH	no	—
GHK17 [GHK17]	20 (resp. $k^3 + k^2 + 4k$)	8 (resp. $k^2 + 2k$)	$O(\lambda)$	2-LIN (resp. k-LIN)	no	—
ADKNO13 [ADK+13]	≥ 40	861	$O(1)$	2-LIN	yes (sym)	√
Ours: $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{asym}}$	4 (resp. $k^2 + 3k$)	7 (resp. $4k + 3$)	$O(\log Q_e)= O(\log \lambda)$	1-LIN = SXDH (resp. k-LIN)	yes (asym)	√
Ours: $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{sym}}$	10 (resp. $k^2 + 3k$)	6 (resp. $2k + 2$)	$O(\log Q_e)= O(\log \lambda)$	2-LIN (resp. k-LIN)	yes (sym)	√

- We provide a generic approach to tightly LR-CCA secure PKE from LR-ardent QAHPS, inheriting the spirit of the Cramer-Shoup HPS paradigm to LR-CCA security [CS02, NS09], but in the multi-challenge setting. Ignoring leakage-resilience, our construction provides a new approach to tightly IND-CCA secure PKE with full compactness, which may be of independent interest.
- We give efficient instantiations based on the matrix DDH (MDDH) assumptions [EHK+13] (which include the standard k-linear (k-LIN) and SXDH assumptions) over asymmetric and symmetric pairing groups, respectively. This results in the most efficient PKE schemes with tight LR-CCA security.

  Specifically, our tightly LR-CCA secure PKE instantiation from SXDH over asymmetric pairing groups has only 4 group elements in the public key and 7 group elements in the ciphertext, hence a couple of hundred times smaller than that of [ADK+13] (which has to be over symmetric pairing groups)[3]. The security loss of LR-CCA security is $O(\log Q_e) = O(\log \lambda)$, where $Q_e = \mathsf{poly}(\lambda)$ denotes the number of encryption queries and λ the security parameter.

In Table 1, we compare our tightly (LR-)CCA secure PKE with existing ones.

1.1 Technical Overview

We firstly recall the Cramer-Shoup paradigm for constructing (LR-)CCA secure PKE [CS02, NS09], explain the difficulty of extending it to the multi-challenge setting, then detail our new approach for designing tightly LR-CCA secure PKE.

The Cramer-Shoup Paradigm: (LR-)CCA Secure PKE from HPS. Hash Proof System (HPS) was originated in [CS02] and can be instantiated from a collection of assumptions. The power of HPS was firstly shown by Cramer and Shoup [CS02], who proposed a paradigm for constructing IND-CCA secure PKE from a smooth-HPS and a universal$_2$ tag-based (labeled) HPS. Naor and Segev [NS09] showed that HPS is a natural candidate for LR-CCA secure PKE, and proved a variant of the Cramer-Shoup PKE scheme to be LR-CCA secure. Over the years, HPS and its variants have demonstrated their charm with a variety of applications in public-key cryptosystem [KD04, ADN+10, Wee12, QL13, FV16], to name a few.

Roughly speaking, an HPS is associated with an NP-language $\mathcal{L} \subseteq \mathcal{X}$ and has two evaluation modes. In the private evaluation mode, the hash value $\Lambda_{sk}(x)$ of an arbitrary $x \in \mathcal{X}$ can be efficiently computed from the hashing key sk and x, i.e., $\mathsf{Priv}(sk, x) = \Lambda_{sk}(x)$; in the public evaluation mode, the hash value $\Lambda_{sk}(x)$ of an instance $x \in \mathcal{L}$ is completely determined by the projection key $pk = \alpha(sk)$, and can

[3] To the best of our knowledge, the PKE scheme in [ADK+13] is the only tightly LR-CCA secure one prior to our work.

be efficiently computed from pk with the help of any witness w for $x \in \mathcal{L}$, i.e., $\mathsf{Pub}(pk, x, w) = \Lambda_{sk}(x)$. The notion of HPS can be generalized to tag-based HPS, where a tag τ serves as an auxiliary input for Λ_{sk}, Pub and Priv.

A typical construction of CCA-secure PKE from a smooth $\mathsf{HPS} = (\Lambda_{(\cdot)}, \alpha, \mathsf{Pub}, \mathsf{Priv})$ and a universal$_2$ tag-based $\widetilde{\mathsf{HPS}} = (\widetilde{\Lambda}_{(\cdot)}, \widetilde{\alpha}, \widetilde{\mathsf{Pub}}, \widetilde{\mathsf{Priv}})$ works as follows [CS02]. The public key contains $pk = \alpha(sk)$ and $\widetilde{pk} = \widetilde{\alpha}(\widetilde{sk})$. The ciphertext is

$$C \;=\; \big(\; x, \;\; d = \mathsf{Pub}(pk, x, w) + M, \;\; \pi = \widetilde{\mathsf{Pub}}(\widetilde{pk}, x, w, \tau) \;\big),$$

where M is a plaintext, $x \leftarrow_{\$} \mathcal{L}$ with witness w and $\tau = \mathsf{H}(x, d)$ with H a collision-resistant hash function. The CCA-security with a single challenge ciphertext $C^* = (x^*, d^*, \pi^*)$ is justified by the following arguments.

(1) By the hardness of the subset membership problem (SMP) related to HPS and $\widetilde{\mathsf{HPS}}$, we can replace $x^* \leftarrow_{\$} \mathcal{L}$ in the challenge ciphertext with $x^* \leftarrow_{\$} \mathcal{X} \setminus \mathcal{L}$, and compute $C^* = \big(x^*,\ d^* = \Lambda_{sk}(x^*) + M,\ \pi^* = \widetilde{\Lambda}_{\widetilde{sk}}(x^*, \tau^*)\big)$.
(2) By the (perfectly) universal$_2$ property of tag-based $\widetilde{\mathsf{HPS}}$, any ill-formed ciphertext $C = \big(x \in \mathcal{X} \setminus \mathcal{L},\ d, \pi'\big)$ results in a uniformly distributed $\pi = \widetilde{\Lambda}_{\widetilde{sk}}(x, \tau)$, even conditioned on $\widetilde{pk} = \widetilde{\alpha}(\widetilde{sk})$ and $\pi^* = \widetilde{\Lambda}_{\widetilde{sk}}(x^*, \tau^*)$. Thus any decryption query on ill-formed ciphertexts will be rejected (due to the fact that $\pi' = \pi$ holds with a negligible probability).
(3) Now the information that the decryption oracle leaks about sk is limited to $pk = \alpha(sk)$. By the smoothness of HPS, $\Lambda_{sk}(x^*)$ involved in the challenge ciphertext is uniformly random conditioned on $pk = \alpha(sk)$, thus it perfectly hides M and the IND-CCA security follows.

LR-CCA security is also easy to achieve since the universal$_2$ property of $\widetilde{\mathsf{HPS}}$ is intrinsically leakage-resilient, and the smoothness of HPS guarantees that $\Lambda_{sk}(x^*)$ still has enough entropy in case of key leakage, then an extractor can be applied to $\Lambda_{sk}(x^*)$ to distill a uniform string to hide M.

Note that the above arguments only apply to the single-challenge setting. In the more realistic setting of multiple challenge ciphertexts, the universal$_2$ property of $\widetilde{\mathsf{HPS}}$ and the smoothness of HPS are too weak to support arguments (2) and (3). More precisely, argument (2) fails since multiple $\{\pi^* = \widetilde{\Lambda}_{\widetilde{sk}}(x^*, \tau^*)\}$ involved in the challenge ciphertexts might leak too much information about $\widetilde{sk}$, and argument (3) fails since the limited entropy contained in sk is not enough to randomize multiple $\{\Lambda_{sk}(x^*)\}$ involved in the challenge ciphertexts. Consequently, one has to resort to a hybrid argument to prove (multi-challenge) (LR-)CCA security, which inevitably introduces a security loss of factor Q_e [BBM00].

Quasi-Adaptive HPS. We provide a novel approach to tightly (LR)-CCA secure PKE in the multi-challenge setting. The core building block in our approach is a new technical tool named *quasi-adaptive HPS (QAHPS)*, which generalizes HPS in a quasi-adaptive setting [JR13]. Different from (traditional) HPS [CS02], QAHPS is associated with a collection $\mathscr{L} = \{\mathcal{L}_\rho\}_\rho$ of NP-languages, and the projection key pk_ρ is allowed to depend on the language $\mathcal{L}_\rho$. In particular, QAHPS possesses a family of projection functions $\alpha_{(\cdot)}$ indexed by a language parameter ρ, so that the action of $\Lambda_{sk}(\cdot)$ on $\mathcal{L}_\rho$ is completely determined by $pk_\rho = \alpha_\rho(sk)$. Intuitively, this allows us to distribute different projection keys for computing hash values of instances from different languages. Tag-based QAHPS can be similarly defined by allowing Λ_{sk}, Pub and Priv to take a tag τ as an auxiliary input.

Our Approach: Tightly LR-CCA Secure PKE from QAHPS. We need three QAHPS schemes for our PKE construction, $\mathsf{QAHPS} = (\Lambda_{(\cdot)}, \alpha_{(\cdot)}, \mathsf{Pub}, \mathsf{Priv})$, $\widehat{\mathsf{QAHPS}} = (\widehat{\Lambda}_{(\cdot)}, \widehat{\alpha}_{(\cdot)}, \widehat{\mathsf{Pub}}, \widehat{\mathsf{Priv}})$ and a tag-based $\widetilde{\mathsf{QAHPS}} = (\widetilde{\Lambda}_{(\cdot)}, \widetilde{\alpha}_{(\cdot)}, \widetilde{\mathsf{Pub}}, \widetilde{\mathsf{Priv}})$. The public key is comprised of $pk_\rho = \alpha_\rho(sk)$, $\widehat{pk}_\rho = \widehat{\alpha}_\rho(\widehat{sk})$ and $\widetilde{pk}_\rho = \widetilde{\alpha}_\rho(\widetilde{sk})$. The ciphertext is

$$\begin{aligned} C &= \big(\; x,\ d = \mathsf{Pub}(pk_\rho, x, w) + M,\ \pi = \widehat{\mathsf{Pub}}(\widehat{pk}_\rho, x, w) + \widetilde{\mathsf{Pub}}(\widetilde{pk}_\rho, x, w, \tau) \;\big) \\ &= \big(\; x,\ d = \Lambda_{sk}(x) + M,\ \pi = \widehat{\pi} + \widetilde{\pi} = \widehat{\Lambda}_{\widehat{sk}}(x) + \widetilde{\Lambda}_{\widetilde{sk}}(x, \tau) \;\big), \end{aligned}$$

where M is a plaintext, $x \leftarrow_{\$} \mathcal{L}_\rho$ with witness w and $\tau = \mathsf{H}(x, d)$ with H a collision-resistant hash function.

For a simple exposition, we first briefly explain why our approach works in the multi-challenge setting and provide a high-level proof of its tight IND-CCA security. Then we show how to extend our approach to leakage-resilient settings.

Intuition of Tight CCA-Security Proof. Similar to the single-challenge (LR-)CCA security proof of the PKE from HPS, our proof goes with three steps.

(1) Replace all $\{x^* \leftarrow_{\$} \mathcal{L}_\rho\}$ in the challenge ciphertexts with $\{x^* \leftarrow_{\$} \mathcal{L}_{\rho_0}\}$.[4] This step is computationally indistinguishable due to the hardness of SMP.
(2) Reject any decryption query on ill-formed ciphertext $C = (x \in \mathcal{X} \setminus \mathcal{L}_\rho,\ d,\ \pi')$.
(3) Replace all $\{\Lambda_{sk}(x^*)\}$ involved in the challenge ciphertexts with uniform strings. Then CCA-security follows.

As shown before, the universal$_2$ and smooth properties are insufficient to support (2) and (3) to achieve tight CCA-security. Thus, stronger properties are needed from QAHPS.

Technical Tool for (2): Ardent QAHPS. We define two statistical properties for QAHPS. Let $\mathscr{L}_0 = \{\mathcal{L}_{\rho_0}\}_{\rho_0}$ and $\mathscr{L}_1 = \{\mathcal{L}_{\rho_1}\}_{\rho_1}$ be two language collections.

- **(Perfectly $\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-Universal).** It demands the uniformity of $\Lambda_{sk}(x)$ conditioned on $\alpha_{\rho_0}(sk)$ and $\alpha_{\rho_1}(sk)$ for any $x \in \mathcal{X} \setminus (\mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1})$, i.e.,

$$\big(\alpha_{\rho_0}(sk),\ \alpha_{\rho_1}(sk),\ \boxed{\Lambda_{sk}(x)}\big) \quad \equiv \quad \big(\alpha_{\rho_0}(sk),\ \alpha_{\rho_1}(sk),\ \boxed{\pi} \leftarrow_{\$} \Pi\big). \tag{1}$$

- **(Perfectly $\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-Key-Switching).** It requires that $\alpha_{\rho_1}(sk)$ can be switched to $\alpha_{\rho_1}(sk')$ for an independent sk' in the presence of $\alpha_{\rho_0}(sk)$, i.e.,

$$\big(\alpha_{\rho_0}(sk),\ \boxed{\alpha_{\rho_1}(sk)}\big) \quad \equiv \quad \big(\alpha_{\rho_0}(sk),\ \boxed{\alpha_{\rho_1}(sk')}\big). \tag{2}$$

It is also reasonable to define $\langle \mathscr{L}, \mathscr{L}_0 \rangle$-universal and $\langle \mathscr{L}, \mathscr{L}_0 \rangle$-key-switching. We call QAHPS enjoying these two kinds of properties a perfectly *ardent QAHPS*. Ardency of QAHPS can be naturally adapted for tag-based QAHPS.

With ardent QAHPS, $\widehat{\mathsf{QAHPS}}$ and tag-based $\widetilde{\mathsf{QAHPS}}$, we describe the high-level idea of justifying (2). By modifying and adapting the latest techniques for proving tight security [GHKP18] (which in turn built upon [GHKW16, Hof17, GHK17]), we partition the ciphertext space economically according to a counter $ctr \in \{1, \cdots, Q_e\}$, which records the serial number of each encryption query issued by the adversary. Taking ctr as a binary string of length $n := \lceil \log Q_e \rceil$, our proof proceeds with n hybrids. In the i-th hybrid, $i \in \{0, 1, \cdots, n\}$, a random function $\mathsf{RF}_i(ctr_{|i})$ on the first i bits of ctr (instead of $\widetilde{sk}$) is employed to compute $\widetilde{\pi}^* = \widetilde{\Lambda}_{\mathsf{RF}_i(ctr_{|i})}(x^*, \tau^*)$ for the challenge ciphertexts; meanwhile, it is also used to compute $\widetilde{\pi} = \widetilde{\Lambda}_{\mathsf{RF}_i(ctr_{|i})}(x, \tau)$ for the decryption of ciphertexts with $x \notin \mathcal{L}_\rho$. In order to go from the i-th hybrid to the $(i+1)$-th hybrid, firstly we replace all $\{x^* \leftarrow_{\$} \mathcal{L}_{\rho_0}\}$ in the challenge ciphertexts with $\{x^* \leftarrow_{\$} \mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1}$ s.t. $x^* \in \mathcal{L}_{\rho_0}$ if $ctr_{i+1} = 0$ and $x^* \in \mathcal{L}_{\rho_1}$ if $ctr_{i+1} = 1\}$; next we employ the ardency of $\widehat{\mathsf{QAHPS}}$ and $\widetilde{\mathsf{QAHPS}}$ to add a dependency of $\mathsf{RF}_i(ctr_{|i})$ on the $(i+1)$-th bit ctr_{i+1} so that $\mathsf{RF}_i(ctr_{|i})$ moves to $\mathsf{RF}_{i+1}(ctr_{|i+1})$, as shown below.

- **($\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-universal forces the instances in decryption queries to fall in $\mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1}$).** By the $\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-universal property of $\widehat{\mathsf{QAHPS}}$, any decryption query on ciphertext with $x \notin \mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1}$ is rejected. The reason is that, the information of $\widehat{sk}$ leaked by the challenge ciphertexts and by the decryption of ciphertexts with $x \in \mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1}$ is limited to $\widehat{\alpha}_{\rho_0}(\widehat{sk})$ and $\widehat{\alpha}_{\rho_1}(\widehat{sk})$.

[4] Here $\mathcal{L}_{\rho_0}$ is from another language collection $\mathscr{L}_0$ and only appears in the security proof. The same is true for $\mathcal{L}_{\rho_1}$ and $\mathscr{L}_1$, as shown later.

- **($\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-key-switching allows the usage of two independent keys for $\mathcal{L}_{\rho_0}$ and $\mathcal{L}_{\rho_1}$).** Note that for $x \in \mathcal{L}_{\rho_0}$, $\widetilde{\pi} = \widetilde{\Lambda}_{\mathsf{RF}_i(ctr_{|i})}(x, \tau)$ is completely determined by $\widetilde{\alpha}_{\rho_0}(\mathsf{RF}_i(ctr_{|i}))$, while for $x \in \mathcal{L}_{\rho_1}$, it is completely determined by $\widetilde{\alpha}_{\rho_1}(\mathsf{RF}_i(ctr_{|i}))$. By the $\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-key-switching property of $\widetilde{\mathsf{QAHPS}}$,

$$\big(\ \widetilde{\alpha}_{\rho_0}(\mathsf{RF}_i(ctr_{|i})),\ \widetilde{\alpha}_{\rho_1}(\mathsf{RF}_i(ctr_{|i}))\ \big) \quad \equiv \quad \big(\ \widetilde{\alpha}_{\rho_0}(\mathsf{RF}_i(ctr_{|i})),\ \widetilde{\alpha}_{\rho_1}(\overline{\mathsf{RF}}_i(ctr_{|i}))\ \big),$$

  where $\overline{\mathsf{RF}}_i$ is an independent random function. Consequently, we can use $\overline{\mathsf{RF}}_i(ctr_{|i})$ to compute $\widetilde{\pi}^*$ for challenge ciphertexts with $x^* \in \mathcal{L}_{\rho_1}$, and to compute $\widetilde{\pi}$ for the decryption of ciphertexts with $x \in \mathcal{L}_{\rho_1}$.

Now we successfully double the entropy in $\mathsf{RF}_i(ctr_{|i})$ to get $\mathsf{RF}_{i+1}(ctr_{|i+1})$ (which equals $\mathsf{RF}_i(ctr_{|i})$ if $ctr_{i+1} = 0$ and $\overline{\mathsf{RF}}_i(ctr_{|i})$ if $ctr_{i+1} = 1$)[5] and this leads us to the $(i+1)$-th hybrid. After n hybrids, for any ill-formed ciphertext with $x \notin \mathcal{L}_{\rho}$, $\widetilde{\pi} = \widetilde{\Lambda}_{\mathsf{RF}_n(ctr)}(x, \tau)$ is fully randomized by $\mathsf{RF}_n(ctr)$, thus the decryption on such ciphertexts will be rejected.

Technical Tool for (3): Multi-Extracting. We define a computational property for QAHPS so that it can amplify the (limited) entropy of a uniform sk to randomize multiple $\{\Lambda_{sk}(x^*)\}$.

- **($\mathscr{L}_0$-Multi-Extracting).** It demands the pseudorandomness of $\Lambda_{sk}(x_j)$ for multiple instances x_j uniformly chosen from $\mathcal{L}_{\rho_0}$, i.e.,

$$\{x_j \leftarrow_\$ \mathcal{L}_{\rho_0}, \boxed{\Lambda_{sk}(x_j)}\}_{j \in [Q_e]} \quad \stackrel{c}{\approx} \quad \{x_j \leftarrow_\$ \mathcal{L}_{\rho_0}, \boxed{\pi_j} \leftarrow_\$ \Pi\}_{j \in [Q_e]}.$$

  By requiring ardent QAHPS to be $\mathscr{L}_0$-multi-extracting, we are able to justify (3). Note that after the change in (2), the decryption oracle might leak $pk_\rho = \alpha_\rho(sk)$ about sk, therefore, the $\mathscr{L}_0$-multi-extracting property is not applicable immediately. We solve this problem by first applying the $\langle \mathscr{L}, \mathscr{L}_0 \rangle$-key-switching property of QAHPS to switch sk to an independent sk' in the computation of $\{\Lambda_{sk'}(x^*)\}$. Under uniform sk', the $\mathscr{L}_0$-multi-extracting property applies and the $\{\Lambda_{sk'}(x^*)\}$ involved in the challenge ciphertexts can be replaced with uniform strings $\{\mathsf{rand}\}$. Then CCA-security follows.

Extension to Tight LR-CCA Security. Like the leakage-resilient PKE [NS09, ADN+10, QL13] from HPS, it is easy to upgrade the tight CCA-security of our PKE construction to tight LR-CCA, as long as the $\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-universal and $\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-key-switching properties of QAHPS holds even if some information $L(sk)$ about sk is leaked. The LR-CCA security proof almost verbatim follows the proof of IND-CCA security. We refer to the main body for more details.

By instantiating leakage-resilient ardent QAHPS over pairing-friendly groups, our approach yields the most efficient tightly LR-CCA secure PKE from the MDDH assumptions, with security loss $O(\log Q_e)$.

1.2 Relation to Existing Techniques for Tight Security

To obtain tight (LR-)CCA security, it is inevitable to implement "consistency check", explicitly or implicitly, to reject decryption queries on ill-formed ciphertexts. In [HJ12, ADK+13, LPJY14, LPJY15, Hof16], a NIZK proof is added in the ciphertext as an explicit consistency check, where NIZK is required to have tight unbounded simulation-soundness (SS) or true-simulation extractability (tSE). Efficient NIZK with tight SS/tSE is very hard to construct, thus leading to large public keys or ciphertexts in these schemes. Gay et al. [GHKW16] implicitly employed a designated-verifier NIZK (DV-NIZK) with tight SS in their construction, which results in large public keys (of over 100 group elements).

[5] Note that for the instance $x^* \in \mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1}$ in challenge ciphertext, the bit indicating whether $x^* \in \mathcal{L}_{\rho_0}$ or $x^* \in \mathcal{L}_{\rho_1}$ is consistent with the $(i+1)$-th bit of ctr, i.e., $x^* \in \mathcal{L}_{\rho_0}$ if $ctr_{i+1} = 0$ and $x^* \in \mathcal{L}_{\rho_1}$ if $ctr_{i+1} = 1$. But this might not be true for the instances $x \in \mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1}$ in the decryption queries. This problem is circumvented by borrowing the trick from [Hof17, GHK17]. We refer to the main body for details.

In order to get more efficient constructions, Hofheinz [Hof17] used *benign proof system* (BPS) as a main technical tool, which is essentially a DV-NIZK with strong soundness, but not as strong as SS. Gay et al. [GHK17] proposed *qualified proof system* (QPS), which is a combination of a DV-NIZK and an HPS. The weak (computational) soundness requirement for QPS enables efficient instantiations, hence resulting in the most compact PKE with tight CCA-security from the DDH assumption over non-pairing groups.

Our construction of PKE employs LR-ardent QAHPS, with LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-universal and LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-key-switching properties. QAHPS can be regarded as a (deterministic) DV-NIZK, and the LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-universal property corresponds to (statistical) soundness which is weaker than BPS but stronger than QPS. Our LR-ardent QAHPS can be instantiated over pairing-friendly groups.

The key leakage-resilience of (QA)HPS enables us to obtain tight LR-CCA security. However, this feature does not apply to the PKE constructions [Hof17, GHK17] from BPS or QPS. For example, the soundness of QPS is a computational notion and might not be justified in the LR settings (cf. Appendix B for the reasons). Thus, the PKE in [GHK17] is unlikely to be tightly LR-CCA secure but is pairing-free, while ours are over pairing-groups but achieve tight LR-CCA security.

2 Preliminaries

Let $\lambda \in \mathbb{N}$ denote the security parameter. For $i, j \in \mathbb{N}$ with $i < j$, define $[i, j] := \{i, i+1, \cdots, j\}$ and $[j] := \{1, 2, \cdots, j\}$. Denote by $x \leftarrow_{\$} \mathcal{X}$ the operation of picking an element x according to a distribution $\mathcal{X}$. If $\mathcal{X}$ is a set, then this denotes that x is sampled uniformly at random from $\mathcal{X}$. For an algorithm $\mathcal{A}$, denote by $y \leftarrow_{\$} \mathcal{A}(x; r)$, or simply $y \leftarrow_{\$} \mathcal{A}(x)$, the operation of running $\mathcal{A}$ with input x and randomness r and assigning the output to y, and by $\mathbf{T}(\mathcal{A})$ the running time of $\mathcal{A}$. "PPT" is short for probabilistic polynomial-time. Denote by poly some polynomial function, and negl some negligible function. For a primitive XX and a security notion YY, we typically denote the advantage of a PPT adversary $\mathcal{A}$ by $\mathsf{Adv}^{\mathrm{YY}}_{\mathrm{XX},\mathcal{A}}(\lambda)$ and define $\mathsf{Adv}^{\mathrm{YY}}_{\mathrm{XX}}(\lambda) := \max_{\mathrm{PPT}\,\mathcal{A}} \mathsf{Adv}^{\mathrm{YY}}_{\mathrm{XX},\mathcal{A}}(\lambda)$. For an $\ell \times k$ matrix $\mathbf{A}$ with $\ell > k$, denote the upper k rows of $\mathbf{A}$ by $\overline{\mathbf{A}}$ and the lower $\ell - k$ rows of $\mathbf{A}$ by $\underline{\mathbf{A}}$. For a string $\tau \in \{0,1\}^\lambda$ and an integer $i \in [0, \lambda]$, denote by $\tau_i \in \{0,1\}$ the i-th bit of τ and $\tau_{|i} \in \{0,1\}^i$ the first i bits of τ. Let ε denote an empty string. For random variables X, Y, Z, let $\Delta(X, Y)$ denote the statistical distance between X and Y, $\Delta(X, Y \,|\, Z)$ a shorthand for $\Delta((X, Z), (Y, Z))$, and $\widetilde{\mathbf{H}}_\infty(X \,|\, Y)$ the average min-entropy of X conditioned on Y. The formal definitions and basic tools are shown in Subsect. 2.1.

2.1 Basic Tools

Let X and Y be two random variables. The min-entropy of X is defined as

$$\mathbf{H}_\infty(X) := -\log(\max_x \Pr[X = x]),$$

and the average min-entropy of X conditioned on Y is defined as

$$\widetilde{\mathbf{H}}_\infty(X \,|\, Y) := -\log\big(\mathbb{E}_{y \leftarrow_{\$} Y}\big[\max_x \Pr[X = x \,|\, Y = y]\big]\big).$$

The statistical distance between X and Y is defined by

$$\Delta(X, Y) := \tfrac{1}{2} \cdot \textstyle\sum_x \big|\Pr[X = x] - \Pr[Y = x]\big|.$$

We use $\Delta(X, Y \,|\, Z)$ as a shorthand for $\Delta((X, Z), (Y, Z))$.

Lemma 1 ([DORS08]). *Let X, Y, Z be three (possibly correlated) random variables. If Z has at most 2^λ possible values, then $\widetilde{\mathbf{H}}_\infty(X \,|\, Y, Z) \geq \widetilde{\mathbf{H}}_\infty(X \,|\, Y) - \lambda$.*

Lemma 2 ([Sho06]). *Let $f : \mathcal{X} \longrightarrow \mathcal{Z}$ be a (possibly randomized) function, and X, Y two random variables on $\mathcal{X}$. Then $\Delta(f(X), f(Y)) \leq \Delta(X, Y)$.*

Definition 1 (Universal Hashing [WC81]). *A family of functions $\mathcal{H} = \{\mathsf{H} : \mathcal{X} \longrightarrow \mathcal{Y}\}$ is called a universal hashing, if for all distinct $x, x' \in \mathcal{X}$, it follows that*

$$\Pr\left[\mathsf{H} \leftarrow_{\$} \mathcal{H} \;:\; \mathsf{H}(x) = \mathsf{H}(x')\right] \;\leq\; 1/|\mathcal{Y}|.$$

Lemma 3 (Generalized Leftover Hash Lemma [DORS08]). *Let $\mathcal{H} = \{\mathsf{H} : \mathcal{X} \longrightarrow \mathcal{Y}\}$ be a family of universal hashing, X a random variable on $\mathcal{X}$ and I a random variable. Then for $\mathsf{H} \leftarrow_{\$} \mathcal{H}$ (where H is independent of X and I) and $U \leftarrow_{\$} \mathcal{Y}$, it holds that*

$$\Delta\big(\ (\mathsf{H},\ \mathsf{H}(X))\ ,\ (\mathsf{H},\ U)\ \big|\ I\ \big) \;\leq\; \sqrt{|\mathcal{Y}| \cdot 2^{-\widetilde{\mathbf{H}}_\infty(X\,|\,I)}}.$$

Next, we develop a specific multi-fold generalized leftover hash lemma. It considers the uniformity of $\mathsf{H}(X_1), \ldots, \mathsf{H}(X_m)$, when a universal hashing H is applied to mutually independent inputs $\{X_j\}_{j\in[m]}$ given not only individual auxiliary variable related to each X_j but also universal auxiliary variable related to all of $\{X_j\}_{j\in[m]}$.

Lemma 4 (Multi-fold Generalized Leftover Hash Lemma). *Let $\mathcal{H} = \{\mathsf{H} : \mathcal{X} \longrightarrow \mathcal{Y}\}$ be a family of universal hashing, $X_1, \cdots, X_m$ mutually independent random variables on $\mathcal{X}$, $f : \mathcal{X} \longrightarrow \mathcal{Z}$ a (possibly randomized) function, and $g : \mathcal{X}^m \longrightarrow \mathcal{W}$ a function. Then for $\mathsf{H} \leftarrow_{\$} \mathcal{H}$ (where H is independent of $X_1, \cdots, X_m$ and f, g) and $U_1, \cdots, U_m \leftarrow_{\$} \mathcal{Y}$, it holds that*

$$\Delta\left(\begin{array}{c} (\mathsf{H},\ \mathsf{H}(X_1),\ \cdots,\ \mathsf{H}(X_m))\ , \\ (\mathsf{H},\ U_1,\ \cdots,\ U_m) \end{array} \;\middle|\; \begin{array}{c} f(X_1), \cdots, f(X_m), \\ g(X_1, \cdots, X_m) \end{array} \right) \leq \sum_{j\in[m]} \sqrt{|\mathcal{Y}| \cdot |\mathcal{Z}| \cdot |\mathcal{W}| \cdot 2^{-\mathbf{H}_\infty(X_j)}}.$$

Proof. It suffices to prove

$$\begin{aligned} \Delta_j := \Delta &\left(\begin{array}{c} (\mathsf{H},\ U_1,\ \cdots,\ U_{j-1},\ \boxed{\mathsf{H}(X_j)},\ \mathsf{H}(X_{j+1}),\ \cdots,\ \mathsf{H}(X_m))\ , \\ (\mathsf{H},\ U_1,\ \cdots,\ U_{j-1},\ \quad \boxed{U_j} \quad,\ \mathsf{H}(X_{j+1}),\ \cdots,\ \mathsf{H}(X_m)) \end{array} \;\middle|\; \begin{array}{c} f(X_1), \cdots, f(X_m), \\ g(X_1, \cdots, X_m) \end{array} \right) \\ &\leq \sqrt{|\mathcal{Y}| \cdot |\mathcal{Z}| \cdot |\mathcal{W}| \cdot 2^{-\mathbf{H}_\infty(X_j)}} \end{aligned} \tag{3}$$

for any $j \in [m]$. Then Lemma 4 follows from the triangle inequality.

Observe that

$$\Delta_j \leq \Delta\left((\mathsf{H},\ \boxed{\mathsf{H}(X_j)})\ , (\mathsf{H},\ \boxed{U_j}) \;\middle|\; \begin{array}{c} X_1,\ \cdots,\ X_{j-1},\ X_{j+1},\ \cdots,\ X_m, \\ f(X_j),\ g(X_1, \cdots, X_m) \end{array} \right) \tag{4}$$

$$\begin{aligned} = &\sum_{x_1,\cdots,x_{j-1},x_{j+1},\cdots,x_m} \Pr\left[(X_1, \cdots, X_{j-1}, X_{j+1}, \cdots, X_m) = (x_1, \cdots, x_{j-1}, x_{j+1}, \cdots, x_m)\right] \\ &\cdot \Delta\big(\ (\mathsf{H},\ \boxed{\mathsf{H}(X_j)})\ ,\ (\mathsf{H},\ \boxed{U_j})\ \big|\ f(X_j),\ g(x_1, \cdots, x_{j-1}, X_j, x_{j+1}, \cdots, x_m)\ \big) \end{aligned} \tag{5}$$

$$\begin{aligned} \leq &\sum_{x_1,\cdots,x_{j-1},x_{j+1},\cdots,x_m} \Pr\left[(X_1, \cdots, X_{j-1}, X_{j+1}, \cdots, X_m) = (x_1, \cdots, x_{j-1}, x_{j+1}, \cdots, x_m)\right] \\ &\cdot \sqrt{|\mathcal{Y}| \cdot 2^{-\widetilde{\mathbf{H}}_\infty(X_j\,|\,f(X_j),\ g(x_1,\cdots,x_{j-1},X_j,x_{j+1},\cdots,x_m))}} \end{aligned} \tag{6}$$

$$\begin{aligned} \leq &\sum_{x_1,\cdots,x_{j-1},x_{j+1},\cdots,x_m} \Pr\left[(X_1, \cdots, X_{j-1}, X_{j+1}, \cdots, X_m) = (x_1, \cdots, x_{j-1}, x_{j+1}, \cdots, x_m)\right] \\ &\cdot \sqrt{|\mathcal{Y}| \cdot 2^{-\left(\mathbf{H}_\infty(X_j) - \log|\mathcal{Z}| - \log|\mathcal{W}|\right)}} \end{aligned} \tag{7}$$

$$= \sqrt{|\mathcal{Y}| \cdot |\mathcal{Z}| \cdot |\mathcal{W}| \cdot 2^{-\mathbf{H}_\infty(X_j)}},$$

where (4) follows from Lemma 2, (5) holds since $(X_1, \cdots, X_{j-1}, X_{j+1}, \cdots, X_m)$ is independent of (H, X_j, U_j), (6) follows from the generalized leftover hash lemma (i.e., Lemma 3), and (7) holds due to Lemma 1.

Therefore, (3) holds and this completes the proof of Lemma 4. □

2.2 Games

Our security proof will consist of game-based security reductions. A game G starts with an Initialize procedure and ends with a Finalize procedure. There are also some optional procedures $\text{Proc}_1, \cdots, \text{Proc}_n$ performing as oracles. All procedures are described using pseudo-code, where initially all variables are empty strings ε and all sets are empty. That an adversary $\mathcal{A}$ is executed in G implies the following procedure: $\mathcal{A}$ first calls Initialize, obtaining the corresponding output; then it may make arbitrary oracle-queries to Proc_i according to their specifications, and obtain their outputs; finally it makes one single call to Finalize. The output of Finalize is called the output of the game G. The symbol "$\Rightarrow$" stands for "Return" in the description of algorithms and procedures. By $\mathsf{G}^{\mathcal{A}} \Rightarrow b$ we mean that G outputs b after interacting with $\mathcal{A}$. By $\Pr_i[\cdot]$ we denote the probability of a particular event occurring in game G_i.

2.3 Public-Key Encryption

A public-key encryption (PKE) scheme $\mathsf{PKE} = (\mathsf{Param}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ consists of a tuple of PPT algorithms: the parameter generation algorithm $\mathsf{PP} \leftarrow_{\$} \mathsf{Param}(1^\lambda)$ outputs a public parameter PP, and we require PP to be an implicit input of other algorithms; the key generation algorithm $(\mathsf{PK}, \mathsf{SK}) \leftarrow_{\$} \mathsf{Gen}(\mathsf{PP})$ outputs a pair of public key PK and secret key SK; the encryption algorithm $C \leftarrow_{\$} \mathsf{Enc}(\mathsf{PK}, M)$ takes as input a public key PK and a message $M \in \mathcal{M}$, and outputs a ciphertext C; the decryption algorithm $M/\bot \leftarrow \mathsf{Dec}(\mathsf{SK}, C)$ takes as input a secret key SK and a ciphertext C, and outputs either a message M or a failure symbol $\bot$. *Perfect correctness* of PKE requires that, for all $\mathsf{PP} \leftarrow_{\$} \mathsf{Param}(1^\lambda)$ and $(\mathsf{PK}, \mathsf{SK}) \leftarrow_{\$} \mathsf{Gen}(\mathsf{PP})$, all messages $M \in \mathcal{M}$, it holds that $\mathsf{Dec}(\mathsf{SK}, \mathsf{Enc}(\mathsf{PK}, M)) = M$.

LR-CCA Security for PKE. Naor and Segev [NS09] defined the leakage-resilient CCA (LR-CCA) security for PKE. In contrast to IND-CCA, the LR-CCA security also allows the adversary $\mathcal{A}$ to make Leak (key leakage) queries adaptively and obtain additional information $L(\mathsf{SK})$ about the secret key SK, where $L : \mathcal{SK} \longrightarrow \{0,1\}^* \setminus \{\varepsilon\}$ is the leakage function submitted by $\mathcal{A}$. According to [NS09], two restrictions are necessary: *(i)* the total amount of leakage bits is *bounded* by some positive integer κ; *(ii)* $\mathcal{A}$ can only access the Leak oracle *before* it obtains a challenge ciphertext (otherwise $\mathcal{A}$ could trivially win by querying the first few bits of $\mathsf{Dec}(\cdot, C^*)$ after receiving a challenge ciphertext C^*).

We present the definition of the κ-leakage-resilient CCA security in its multi-ciphertext version. The leakage-rate of the LR-CCA security is defined as the ratio of κ to the bit-length of secret key, i.e., $\kappa/\mathsf{BitLength}(\mathsf{SK})$.

Definition 2 (Multi-Ciphertext κ-Leakage-Resilient CCA Security). *Let $\kappa = \kappa(\lambda)$. A PKE scheme PKE is κ-LR-CCA secure, if for any PPT adversary $\mathcal{A}$, it holds that*

$$\mathsf{Adv}^{\kappa\text{-}lr\text{-}cca}_{\mathsf{PKE},\mathcal{A}}(\lambda) := \left| \Pr[\kappa\text{-}\mathsf{lr}\text{-}\mathsf{cca}^{\mathcal{A}} \Rightarrow 1] - \tfrac{1}{2} \right| \le \mathsf{negl}(\lambda),$$

where game κ-lr-cca is specified in Fig. 1.

If $\kappa = 0$, κ-LR-CCA security is reduced to the traditional IND-CCA security.

Proc. Initialize: $\mathsf{PP} \leftarrow_{\$} \mathsf{Param}(1^\lambda)$. $(\mathsf{PK}, \mathsf{SK}) \leftarrow_{\$} \mathsf{Gen}(\mathsf{PP})$. $\beta \leftarrow_{\$} \{0,1\}$. // challenge bit $l := 0$. // bit length of leakage $\mathsf{chal} := \mathsf{false}$. Return $(\mathsf{PP}, \mathsf{PK})$.	**Proc.** Leak(L): If $(\mathsf{chal} = \mathsf{true})$ $\vee\ (l + \lvert L(\mathsf{SK})\rvert > \kappa)$, Return $\bot$. $l := l + \lvert L(\mathsf{SK})\rvert$. Return $L(\mathsf{SK})$.	**Proc.** Enc(M_0, M_1): $\mathsf{chal} := \mathsf{true}$. If $\lvert M_0\rvert \ne \lvert M_1\rvert$, Return $\bot$. $C^* \leftarrow_{\$} \mathsf{Enc}(\mathsf{PK}, M_\beta)$. $\mathcal{Q}_{\mathcal{ENC}} := \mathcal{Q}_{\mathcal{ENC}} \cup \{C^*\}$. Return C^*.	**Proc.** Dec(C): If $C \in \mathcal{Q}_{\mathcal{ENC}}$, Return $\bot$. Return $\mathsf{Dec}(\mathsf{SK}, C)$. **Proc.** Finalize$(\beta')$: Return $(\beta' = \beta)$.

Fig. 1. κ-lr-cca security game for PKE, where $\lvert L(\mathsf{SK})\rvert$ denotes the bit length of $L(\mathsf{SK})$.

2.4 Pairing Groups

Let $\mathsf{PGGen}(1^\lambda)$ be a PPT algorithm outputting a description of pairing group $\mathcal{PG} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, e, P_1, P_2, P_T)$, where $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ are additive cyclic groups of order p, p is a prime number of bit-length at least λ, $e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$ is a non-degenerated bilinear pairing, and P_1, P_2, P_T are generators of $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$, respectively, with $P_T := e(P_1, P_2)$. We assume that the operations in $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$ and the pairing e are efficiently computable. We require the pairing group $\mathcal{PG}$ to be an implicit input of other algorithms.

We use the implicit representation of group elements following [EHK+13]. For a matrix $\mathbf{A} = (a_{i,j})$ over $\mathbb{Z}_p$, denote by $[\mathbf{A}]_s := (a_{i,j} \cdot P_s)$ the implicit representation of $\mathbf{A}$ in $\mathbb{G}_s$ (which may be $\mathbb{G}_1$, $\mathbb{G}_2$, or $\mathbb{G}_T$). Clearly, given $\mathbf{A}$, $[\mathbf{B}]_s$, $[\mathbf{C}]_s$ and $\mathbf{D}$ with composable dimensions, one can efficiently compute $[\mathbf{AB}]_s$, $[\mathbf{B}+\mathbf{C}]_s$, $[\mathbf{CD}]_s$; given $[\mathbf{A}]_1$ and $[\mathbf{B}]_2$, one can efficiently compute $[\mathbf{AB}]_T$ with the pairing e.

$\mathcal{PG}$ is said to be a *Type-I symmetric pairing group* if $\mathbb{G}_1 = \mathbb{G}_2$. In this case, we let $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$ and $P_1 = P_2 = P$, abbreviate $\mathcal{PG} = (\mathbb{G}, \mathbb{G}_T, p, e, P, P_T)$, and denote $[\mathbf{A}]_1 = [\mathbf{A}]_2 = [\mathbf{A}]$. $\mathcal{PG}$ is said to be a *Type-III asymmetric pairing group* if $\mathbb{G}_1 \neq \mathbb{G}_2$, and there does not exist an efficiently computable isomorphism between $\mathbb{G}_1$ and $\mathbb{G}_2$.

Let $\ell, k \geq 1$ be integers with $\ell > k$. A probabilistic distribution $\mathcal{D}_{\ell,k}$ is called a *matrix distribution*, if it outputs matrices in $\mathbb{Z}_p^{\ell \times k}$ of full rank k in polynomial time. Without loss of generality, we assume that the first k rows of $\mathbf{A} \leftarrow_\$ \mathcal{D}_{\ell,k}$ are linearly independent. Let $\mathcal{D}_k := \mathcal{D}_{k+1,k}$. Denote by $\mathcal{U}_{\ell,k}$ the *uniform distribution* over all matrices in $\mathbb{Z}_p^{\ell \times k}$. Let $\mathcal{U}_k := \mathcal{U}_{k+1,k}$. We review the Matrix DDH (MDDH) and Q-fold MDDH assumptions relative to PGGen, as well as the random self-reducibility of the MDDH assumptions below.

The $\mathcal{D}_{\ell,k}$-Matrix DDH ($\mathcal{D}_{\ell,k}$-MDDH) problem over group $\mathbb{G}_s$ (which may be $\mathbb{G}_1$ or $\mathbb{G}_2$), is to distinguish the two distributions $([\mathbf{A}]_s, [\mathbf{Aw}]_s)$ and $([\mathbf{A}]_s, [\mathbf{u}]_s)$. The distinguishing advantage of an adversary $\mathcal{A}$ is denoted by

$$\mathsf{Adv}^{mddh}_{\mathcal{D}_{\ell,k},\mathbb{G}_s,\mathcal{A}}(\lambda) := |\Pr[\mathcal{A}([\mathbf{A}]_s, [\mathbf{Aw}]_s) = 1] - \Pr[\mathcal{A}([\mathbf{A}]_s, [\mathbf{u}]_s) = 1]|,$$

where $\mathbf{A} \leftarrow_\$ \mathcal{D}_{\ell,k}$, $\mathbf{w} \leftarrow_\$ \mathbb{Z}_p^k$ and $\mathbf{u} \leftarrow_\$ \mathbb{Z}_p^\ell$. The $\mathcal{D}_{\ell,k}$-MDDH assumption over $\mathbb{G}_s$ assumes that for all PPT adversaries $\mathcal{A}$, $\mathsf{Adv}^{mddh}_{\mathcal{D}_{\ell,k},\mathbb{G}_s,\mathcal{A}}(\lambda)$ is negligible.

The MDDH assumption covers many well-studied assumptions, such as the DDH and the k-LIN assumptions, by specifying the matrix distribution as $\mathcal{LIN}_1$ and $\mathcal{LIN}_k$ respectively [EHK+13], where

$$\mathcal{LIN}_k: \ \mathbf{A} = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_k \\ 1 & \cdots & 1 \end{pmatrix} \in \mathbb{Z}_p^{(k+1)\times k}.$$

Several relations among MDDH assumptions w.r.t. different matrix distributions were established in [EHK+13, GHKW16].

Lemma 5 ($\mathcal{D}_{\ell,k}$-MDDH $\Rightarrow$ $\mathcal{U}_k$-MDDH [EHK+13] $\Rightarrow$ $\mathcal{U}_{\ell,k}$-MDDH [GHKW16]). *For any adversary $\mathcal{A}$, there exists an adversary $\mathcal{B}$ such that $\mathbf{T}(\mathcal{B}) \approx \mathbf{T}(\mathcal{A})$ and*

$$\mathsf{Adv}^{mddh}_{\mathcal{U}_k,\mathbb{G}_s,\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{mddh}_{\mathcal{D}_{\ell,k},\mathbb{G}_s,\mathcal{B}}(\lambda).$$

For any adversary $\mathcal{A}$, there exists an adversary $\mathcal{B}$ such that $\mathbf{T}(\mathcal{B}) \approx \mathbf{T}(\mathcal{A})$ and

$$\mathsf{Adv}^{mddh}_{\mathcal{U}_{\ell,k},\mathbb{G}_s,\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{mddh}_{\mathcal{U}_k,\mathbb{G}_s,\mathcal{B}}(\lambda).$$

Consequently, for any $\ell > k$, $\mathcal{U}_{\ell,k}$-MDDH assumption is tightly implied by the k-LIN assumption (i.e., $\mathcal{LIN}_k$-MDDH).

For $Q \geq 1$, consider the Q-fold $\mathcal{D}_{\ell,k}$-MDDH problem over group $\mathbb{G}_s$, which is to distinguish two distributions $([\mathbf{A}]_s, [\mathbf{AW}]_s)$ and $([\mathbf{A}]_s, [\mathbf{U}]_s)$. The distinguishing advantage of an adversary $\mathcal{A}$ is denoted by

$$\mathsf{Adv}^{Q\text{-}mddh}_{\mathcal{D}_{\ell,k},\mathbb{G}_s,\mathcal{A}}(\lambda) := |\Pr[\mathcal{A}([\mathbf{A}]_s, [\mathbf{AW}]_s) = 1] - \Pr[\mathcal{A}([\mathbf{A}]_s, [\mathbf{U}]_s) = 1]|,$$

where $\mathbf{A} \leftarrow_\$ \mathcal{D}_{\ell,k}$, $\mathbf{W} \leftarrow_\$ \mathbb{Z}_p^{k\times Q}$ and $\mathbf{U} \leftarrow_\$ \mathbb{Z}_p^{\ell\times Q}$. The Q-fold $\mathcal{D}_{\ell,k}$-MDDH assumption over $\mathbb{G}_s$ assumes that for all PPT adversaries $\mathcal{A}$, $\mathsf{Adv}^{Q\text{-}mddh}_{\mathcal{D}_{\ell,k},\mathbb{G}_s,\mathcal{A}}(\lambda)$ is negligible.

$\mathcal{D}_{\ell,k}$-MDDH problem is random self-reducible [EHK+13], so Q-fold and (1-fold) $\mathcal{D}_{\ell,k}$-MDDH problems can be tightly reduced to each other. In particular, for the uniform distribution $\mathcal{U}_{\ell,k}$, the reduction is even tighter.

Lemma 6 (Random Self-Reducibility of $\mathcal{D}_{\ell,k}$-MDDH & $\mathcal{U}_{\ell,k}$-MDDH [EHK+13]). *Let $Q > \ell - k$. For any adversary $\mathcal{A}$, there exists an adversary $\mathcal{B}$, such that $\mathbf{T}(\mathcal{B}) \approx \mathbf{T}(\mathcal{A}) + Q \cdot \mathsf{poly}(\lambda)$ with $\mathsf{poly}(\lambda)$ independent of $\mathbf{T}(\mathcal{A})$, and*

$$\mathsf{Adv}^{Q\text{-}mddh}_{\mathcal{D}_{\ell,k},\mathbb{G}_s,\mathcal{A}}(\lambda) \le (\ell - k) \cdot \mathsf{Adv}^{mddh}_{\mathcal{D}_{\ell,k},\mathbb{G}_s,\mathcal{B}}(\lambda) + 1/(p-1).$$

For any adversary $\mathcal{A}$, there exists an adversary $\mathcal{B}$, such that $\mathbf{T}(\mathcal{B}) \approx \mathbf{T}(\mathcal{A}) + Q \cdot \mathsf{poly}(\lambda)$ with $\mathsf{poly}(\lambda)$ independent of $\mathbf{T}(\mathcal{A})$, and

$$\mathsf{Adv}^{Q\text{-}mddh}_{\mathcal{U}_{\ell,k},\mathbb{G}_s,\mathcal{A}}(\lambda) \le \mathsf{Adv}^{mddh}_{\mathcal{U}_{\ell,k},\mathbb{G}_s,\mathcal{B}}(\lambda) + 1/(p-1).$$

2.5 Collision-Resistant Hashing

Definition 3 (Collision-Resistant Hashing). *A family of functions $\mathcal{H} = \{\mathsf{H} : \mathcal{X} \longrightarrow \mathcal{Y}\}$ is collision-resistant, if for any PPT adversary $\mathcal{A}$, it holds that*

$$\mathsf{Adv}^{cr}_{\mathcal{H},\mathcal{A}}(\lambda) := \Pr\left[\mathsf{H} \leftarrow_\$ \mathcal{H},\ (x, x') \leftarrow_\$ \mathcal{A}(\mathsf{H})\ :\ \mathsf{H}(x) = \mathsf{H}(x')\ \wedge\ x \neq x'\right] \le \mathsf{negl}(\lambda).$$

3 Quasi-Adaptive HPS: Ardency and Leakage Resilience

For hash proof system (HPS) defined in [CS02], the associated NP-language $\mathcal{L}$ is generated in the setup phase once and for all, and the projection key pk is used for computing hash values of instances in this fixed $\mathcal{L}$.

In this section, we formalize the notion of *quasi-adaptive HPS (QAHPS)*,[6] which is associated with a collection $\mathscr{L} = \{\mathcal{L}_\rho\}_\rho$ of NP-languages. Different from HPS, the projection key pk_ρ of QAHPS is allowed to depend on the specific language $\mathcal{L}_\rho$ for which hash values are computed.

As the main technical novelty, we propose two new statistical properties for QAHPS, including *κ-LR-$\langle\mathscr{L}_0, \mathscr{L}_1\rangle$-universal* and *$\kappa$-LR-$\langle\mathscr{L}_0, \mathscr{L}_1\rangle$-key-switching*. This type of QAHPS is termed as *LR-ardent QAHPS*. We also define the tag-based version of QAHPS and adapt the notion of LR-ardency for it. LR-ardent QAHPS and tag-based one will serve as our core technical tools.

3.1 Language Distribution

In this subsection, we formalize the collection of NP-languages, with which a QAHPS is associated, as a language distribution.

Definition 4 (Language Distribution). *A language distribution $\mathscr{L}$ is a probability distribution that outputs a language parameter ρ as well as a trapdoor td in polynomial time. The language parameter ρ publicly defines an NP-language $\mathcal{L}_\rho \subseteq \mathcal{X}_\rho$. For simplicity, we assume that the universe $\mathcal{X}_\rho$ is the same for all languages $\mathcal{L}_\rho$, denoted by $\mathcal{X}$. The trapdoor td is required to contain enough information for deciding whether or not an instance $x \in \mathcal{X}$ is in $\mathcal{L}_\rho$. We require that there are PPT algorithms for sampling $x \leftarrow_\$ \mathcal{L}_\rho$ uniformly together with a witness w and sampling $x \leftarrow_\$ \mathcal{X}$ uniformly.*

We define a subset membership problem (SMP) for a language distribution $\mathscr{L}$, which asks whether an element is uniformly chosen from $\mathcal{L}_\rho$ or $\mathcal{X}$.

[6] Quasi-adaptiveness of HPS was discussed in [JR15]. Here we give a formal definition of QAHPS and build our novel LR-ardency notion over it.

Definition 5 (Subset Membership Problem). *The subset membership problem (SMP) related to a language distribution $\mathscr{L}$ is hard, if for any PPT adversary $\mathcal{A}$, it holds that*

$$\mathsf{Adv}^{smp}_{\mathscr{L},\mathcal{A}}(\lambda) := |\Pr[\mathcal{A}(\rho, x) = 1] - \Pr[\mathcal{A}(\rho, x') = 1]| \leq \mathsf{negl}(\lambda),$$

where $(\rho, td) \leftarrow_{\$} \mathscr{L}$, $x \leftarrow_{\$} \mathcal{L}_\rho$ and $x' \leftarrow_{\$} \mathcal{X}$.

We also define a multi-fold version of SMP, which is to distinguish multiple instances, all of which are uniformly chosen either from $\mathcal{L}_\rho$ or from $\mathcal{X}$.

Definition 6 (Multi-fold SMP). *The multi-fold SMP related to a language distribution $\mathscr{L}$ is hard, if for any PPT adversary $\mathcal{A}$, any polynomial $Q = \mathsf{poly}(\lambda)$, it holds that*

$$\mathsf{Adv}^{Q\text{-}msmp}_{\mathscr{L},\mathcal{A}}(\lambda) := \left|\Pr\left[\mathcal{A}(\rho, \{x_j\}_{j\in[Q]}) = 1\right] - \Pr\left[\mathcal{A}(\rho, \{x'_j\}_{j\in[Q]}) = 1\right]\right| \leq \mathsf{negl}(\lambda)$$

where $(\rho, td) \leftarrow_{\$} \mathscr{L}$, $x_1, \cdots, x_Q \leftarrow_{\$} \mathcal{L}_\rho$ and $x'_1, \cdots, x'_Q \leftarrow_{\$} \mathcal{X}$.

By a standard hybrid argument, SMP and multi-fold SMP are equivalent. For some language distributions, such as those for linear subspaces (cf. Subsect. 5.2), the hardness of multi-fold SMP can be tightly reduced to that of SMP.

3.2 Quasi-Adaptive HPS

Definition 7 (Quasi-Adaptive Hash Proof System). *A quasi-adaptive hash proof system (QAHPS)* $\mathsf{QAHPS} = (\mathsf{Setup}, \alpha_{(\cdot)}, \mathsf{Pub}, \mathsf{Priv})$ *for a language distribution $\mathscr{L}$ consists of a tuple of PPT algorithms:*

- *$pp \leftarrow_{\$} \mathsf{Setup}(1^\lambda)$: The setup algorithm outputs a public parameter pp, which implicitly defines $(\mathcal{SK}, \Pi, \Lambda_{(\cdot)})$, where*
  - *$\mathcal{SK}$ is the hashing key space and Π is the hash value space;*
  - *$\Lambda_{(\cdot)} : \mathcal{X} \longrightarrow \Pi$ is a family of hash functions indexed by a hashing key $sk \in \mathcal{SK}$, where $\mathcal{X}$ is the universe for languages output by $\mathscr{L}$.*

  We assume that $\Lambda_{(\cdot)}$ is efficiently computable and there are PPT algorithms for sampling $sk \leftarrow_{\$} \mathcal{SK}$ uniformly and sampling $\pi \leftarrow_{\$} \Pi$ uniformly. We require pp to be an implicit input of other algorithms.
- *$pk_\rho \leftarrow \alpha_\rho(sk)$: The projection algorithm outputs a projection key pk_ρ of hashing key $sk \in \mathcal{SK}$ w.r.t. the language parameter ρ.*
- *$\pi \leftarrow \mathsf{Pub}(pk_\rho, x, w)$: The public evaluation algorithm outputs the hash value $\pi = \Lambda_{sk}(x) \in \Pi$ of $x \in \mathcal{L}_\rho$, with the help of the projection key $pk_\rho = \alpha_\rho(sk)$ specified by ρ and a witness w for $x \in \mathcal{L}_\rho$.*
- *$\pi \leftarrow \mathsf{Priv}(sk, x)$: The private evaluation algorithm outputs the hash value $\pi = \Lambda_{sk}(x) \in \Pi$ of $x \in \mathcal{X}$, directly using the hashing key sk.*

Perfect correctness (a.k.a. projectiveness) of QAHPS *requires that, for all possible $pp \leftarrow_{\$} \mathsf{Setup}(1^\lambda)$ and $(\rho, td) \leftarrow_{\$} \mathscr{L}$, all hashing keys $sk \in \mathcal{SK}$ with $pk_\rho = \alpha_\rho(sk)$ the corresponding projection key w.r.t. ρ, all $x \in \mathcal{L}_\rho$ with all possible witnesses w, it holds that*

$$\mathsf{Pub}(pk_\rho, x, w) \;=\; \Lambda_{sk}(x) \;=\; \mathsf{Priv}(sk, x).$$

Remark 1 (Relation to HPS). In contrast to the HPS defined by Cramer and Shoup [CS02] (cf. Definition 14 in Appendix A.2), there are two main differences:

- Instead of a single language, QAHPS is associated with a collection of languages $\mathscr{L} = \{\mathcal{L}_\rho\}_\rho$ characterized by a language distribution. In particular, the specific language $\mathcal{L}_\rho$ is no longer generated in the setup phase Setup.
- Instead of a single projection function, QAHPS possesses a family of projection functions $\alpha_{(\cdot)} : \mathcal{SK} \longrightarrow \mathcal{PK}_{(\cdot)}$ indexed by a language parameter ρ, so that the action of $\Lambda_{sk}(\cdot)$ on $\mathcal{L}_\rho$ is completely determined by $pk_\rho := \alpha_\rho(sk)$.

In a nutshell, the relation between HPS and QAHPS is analogous to the relation between NIZK and QA-NIZK [JR13].

Remark 2 (Relation to DV-QA-NIZK). An HPS is essentially a (deterministic) designated-verifier non-interactive zero-knowledge (DV-NIZK) proof system [GHKW16]. Similarly, our QAHPS can be viewed as a (deterministic) DV-QA-NIZK.

Dodis et al. [DKPW12] defined an extracting property for (traditional) HPS, which requires the hash value $\Lambda_{sk}(x)$ to be uniformly distributed over Π for any $x \in \mathcal{X}$, as long as sk is uniformly chosen from $\mathcal{SK}$. Intuitively, $\Lambda_{(\cdot)}(x)$ acts as an extractor and extracts the entropy from sk. Here, we introduce a *computational* analogue of the extracting property in a *multi-fold* version for QAHPS, called *multi-extracting property*, which demands the pseudorandomness of $\Lambda_{sk}(x_j)$ for multiple instances x_j, $j \in [Q]$.

Definition 8 ($\mathscr{L}_0$-Multi-Extracting QAHPS). *Let $\mathscr{L}_0$ be a language distribution (which might be different from $\mathscr{L}$).* QAHPS *for $\mathscr{L}$ is called $\mathscr{L}_0$-multi-extracting, if for any PPT adversary $\mathcal{A}$, any $Q = \mathsf{poly}(\lambda)$, the following advantage is negligible*

$$\mathsf{Adv}^{Q\text{-}\mathscr{L}_0\text{-}mext}_{\mathsf{QAHPS},\mathcal{A}}(\lambda) := \Big|\Pr\big[\mathcal{A}\big(pp, \rho_0, \{x_j, \boxed{\Lambda_{sk}(x_j)}\}_{j\in[Q]}\big) = 1\big] - \Pr\big[\mathcal{A}\big(pp, \rho_0, \{x_j, \boxed{\pi_j}\}_{j\in[Q]}\big) = 1\big]\Big|,$$

where $pp \leftarrow_\$ \mathsf{Setup}(1^\lambda)$, $(\rho_0, td_0) \leftarrow_\$ \mathscr{L}_0$, $sk \leftarrow_\$ \mathcal{SK}$, $x_1, \cdots, x_Q \leftarrow_\$ \mathcal{L}_{\rho_0}$, and $\pi_1, \cdots, \pi_Q \leftarrow_\$ \Pi$.

We note that the $\mathscr{L}_0$-multi-extracting property is defined in an *average-case* flavor, i.e., the instances x_j, $j \in [Q]$, are uniformly chosen from $\mathcal{L}_{\rho_0}$.

3.3 Ardent QAHPS with Leakage Resilience

In this subsection, we introduce two statistical properties for QAHPS, including κ-LR-$\langle\mathscr{L}_0, \mathscr{L}_1\rangle$-universal and κ-LR-$\langle\mathscr{L}_0, \mathscr{L}_1\rangle$-key-switching. These two properties are formalized in a general manner and are parameterized by $\kappa \in \mathbb{N}$ and two language distributions $\langle\mathscr{L}_0, \mathscr{L}_1\rangle$. We name QAHPS enjoying these properties as *LR-ardent* QAHPS. We highlight the leakage $L(sk)$ with gray boxes, in order to show the difference from the perfectly ardent QAHPS as stated in Subsect. 1.1.

Definition 9 (Leakage-Resilient Ardent QAHPS). *Let $\kappa = \kappa(\lambda) \in \mathbb{N}$, and let $\mathscr{L}_0, \mathscr{L}_1$ be a pair of language distributions. A QAHPS scheme* QAHPS *for a language distribution $\mathscr{L}$ is called κ-leakage-resilient $\langle\mathscr{L}_0, \mathscr{L}_1\rangle$-ardent ($\kappa$-LR-$\langle\mathscr{L}_0, \mathscr{L}_1\rangle$-ardent), if the following two properties hold:*

- **(κ-LR-$\langle\mathscr{L}_0, \mathscr{L}_1\rangle$-Universal).** *With probability $1 - 2^{-\Omega(\lambda)}$ over $pp \leftarrow_\$ \mathsf{Setup}(1^\lambda)$, $(\rho_0, td_0) \leftarrow_\$ \mathscr{L}_0$ and $(\rho_1, td_1) \leftarrow_\$ \mathscr{L}_1$, for all $x \in \mathcal{X} \setminus (\mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1})$ and all leakage functions $L : \mathcal{SK} \longrightarrow \{0,1\}^\kappa$, if $sk \leftarrow_\$ \mathcal{SK}$, then*
$$\widetilde{\mathbf{H}}_\infty\big(\Lambda_{sk}(x) \bigm| \alpha_{\rho_0}(sk),\ \alpha_{\rho_1}(sk),\ \boxed{L(sk)}\big) \ \geq\ \Omega(\lambda). \tag{8}$$
We require the inequality to hold for adaptive choices of x and L, where x and L can arbitrarily depend on ρ_0, ρ_1, $\alpha_{\rho_0}(sk)$, $\alpha_{\rho_1}(sk)$.
- **(κ-LR-$\langle\mathscr{L}_0, \mathscr{L}_1\rangle$-Key-Switching).** *With overwhelming probability $1-2^{-\Omega(\lambda)}$ over $pp \leftarrow_\$ \mathsf{Setup}(1^\lambda)$ and $(\rho_0, td_0) \leftarrow_\$ \mathscr{L}_0$, for all leakage functions $L : \mathcal{SK} \longrightarrow \{0,1\}^\kappa$, it holds that:*
$$\Delta\Big(\ \big(\rho_1,\ \boxed{\alpha_{\rho_1}(sk)}\big)\ ,\ \big(\rho_1,\ \boxed{\alpha_{\rho_1}(sk')}\big)\ \Bigm|\ \alpha_{\rho_0}(sk),\ \boxed{L(sk)}\ \Big)\ \leq\ 2^{-\Omega(\lambda)}, \tag{9}$$
where the probability is over $sk, sk' \leftarrow_\$ \mathcal{SK}$ and $(\rho_1, td_1) \leftarrow_\$ \mathscr{L}_1$. We require the inequality to hold for L that is arbitrarily dependent on ρ_0, $\alpha_{\rho_0}(sk)$. However, L is required to be independent of ρ_1.

When $\kappa = 0$, the term "κ-LR" is omitted from these properties. The parameter $\langle\mathscr{L}_0, \mathscr{L}_1\rangle$ is also omitted when it is clear from context.

Remark 3. In the above definition, the public parameter pp is implicitly included in the conditions in (8) and (9). Meanwhile, $\mathscr{L}_0, \mathscr{L}_1$ implicitly take pp as an input.

Remark 4 (Game-Based Definition for LR-Ardency). The definition of LR-ardency goes with a concise style which is consistent with the definition of perfectly ardent QAHPS as shown in Eqs. (1) and (2) in Subsect. 1.1. It can also be formalized via games. Appendix C shows the game-based definition which is more friendly to our security proof of LR-CCA security.

Definition 10 (Ardent QAHPS). QAHPS *is called* $\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$*-ardent if it is* 0*-leakage-resilient* $\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$*-ardent.*

Furthermore, if (8) and (9) are replaced by (1) and (2), then it is **perfectly $\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-universal and key-switching** which is obviously (0-LR-)$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-universal and key-switching. Observe that, perfectly universal property itself carries leakage-resilience to some extent as shown in Lemma 7.

Lemma 7 (Perfectly $\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-Universal $\Rightarrow$ LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-Universal). *If a QAHPS scheme is perfectly* $\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$*-universal, then it is* κ*-LR-*$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$*-universal for any* $\kappa \le \log |\Pi| - \Omega(\lambda)$*, where* Π *is the hash value space of QAHPS.*

Proof. Suppose that QAHPS is perfectly $\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-universal. Then by (1), for all $x \in \mathcal{X} \setminus (\mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1})$, we have:

$$\widetilde{\mathbf{H}}_\infty\big(\Lambda_{sk}(x) \bigm| \alpha_{\rho_0}(sk),\ \alpha_{\rho_1}(sk)\big) \ = \ \log |\Pi|,$$

where $sk \leftarrow_\$ \mathcal{SK}$. Note that, x can arbitrarily depend on sk. Since $L(sk)$ has at most 2^κ possible values, by Lemma 1,

$$\widetilde{\mathbf{H}}_\infty\big(\Lambda_{sk}(x) \bigm| \alpha_{\rho_0}(sk),\ \alpha_{\rho_1}(sk),\ L(sk)\big) \ \ge\ \widetilde{\mathbf{H}}_\infty\big(\Lambda_{sk}(x) \bigm| \alpha_{\rho_0}(sk),\ \alpha_{\rho_1}(sk)\big) - \kappa,$$

which is $\Omega(\lambda)$ for $\kappa \le \log |\Pi| - \Omega(\lambda)$. This completes the proof of Lemma 7. □

Remark 5 (On the Independence between $L(\cdot)$ and ρ_1). We stress that, in the definition of κ-LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-key-switching, the independence between the leakage function $L(\cdot)$ and the language parameter ρ_1 is necessary. Otherwise, this property is unsatisfiable by simply taking $L(\cdot)$ as the first κ bits of $\alpha_{\rho_1}(\cdot)$.

Remark 6 (On the Choices of $\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$). We stress that, in the above definition, $\mathscr{L}_0$ or $\mathscr{L}_1$ is allowed to be $\mathscr{L}$ itself. In particular, it is reasonable to define κ-LR-$\langle \mathscr{L}, \mathscr{L}_0 \rangle$-ardency for a QAHPS scheme QAHPS for $\mathscr{L}$. Besides, we note that κ-LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-universal is identical to κ-LR-$\langle \mathscr{L}_1, \mathscr{L}_0 \rangle$-universal.

Remark 7 (Relation to the Universal$_1$, Universal$_2$ and Extracting Properties). The $\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-universal property of QAHPS generalizes the currently available universal and extracting properties of (traditional) HPS. With different choices of $\mathscr{L}_0$ and $\mathscr{L}_1$, it will turn into the universal$_1$, the universal$_2$ and the extracting properties of HPS defined in [CS02, DKPW12], respectively.

More precisely, let $\mathscr{L}_\perp$ (or simply $\perp$) denote a special *empty* language distribution, which always outputs $\rho_\perp$ defining the empty language $\mathcal{L}_{\rho_\perp} = \{\}$, and let $\mathscr{L}_{\text{sing}}$ denote a special *singleton* language distribution, which samples $x \leftarrow_\$ \mathcal{X}$ uniformly and outputs ρ_x defining a singleton language $\mathcal{L}_{\rho_x} = \{x\}$. We assume that $\alpha_{\rho_\perp}(sk) = \perp$ and $\alpha_{\rho_x}(sk) = \Lambda_{sk}(x)$ hold for any $sk \in \mathcal{SK}$ and $x \in \mathcal{X}$, both of which are very natural and are satisfied by our instantiations in Sect. 5 and Sect. 6. Then: *(i)* $\langle \mathscr{L}, \perp \rangle$-universal corresponds to the average-case universal$_1$ property; *(ii)* $\langle \mathscr{L}, \mathscr{L}_{\text{sing}} \rangle$-universal corresponds to the average-case universal$_2$ property; *(iii)* Perfectly $\langle \perp, \perp \rangle$-universal corresponds to the extracting property.

The leakage-resilient ardency of QAHPS can be adapted to a weak version.

Definition 11 (Leakage-Resilient Weak-Ardent QAHPS). *Let* $\kappa = \kappa(\lambda) \in \mathbb{N}$*, and let* $\mathscr{L}_0, \mathscr{L}_1$ *be a pair of language distributions. A QAHPS scheme* QAHPS *for a language distribution* $\mathscr{L}$ *is called* κ*-leakage-resilient* $\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$*-weak-ardent (*$\kappa$*-LR-*$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$*-weak-ardent), if* QAHPS *is* $\langle \perp, \perp \rangle$*-universal and supports* κ*-LR-*$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$*-key-switching. Similarly,* $\kappa = 0$ *leads to* **weak-ardent QAHPS**.

3.4 Extension to the Tag-Based Setting

The notion of (traditional) HPS was generalized to extended HPS (a.k.a. labeled HPS) in [CS02] and tag-based HPS in [QLC15], respectively, by allowing the hash functions $\Lambda_{(\cdot)}$ to have an additional element called label/tag as input.

Similarly, in a tag-based QAHPS, the public parameter pp also implicitly defines a tag space $\mathcal{T}$. Meanwhile, the hash functions $\Lambda_{(\cdot)}$, the public evaluation algorithm Pub and the private evaluation algorithm Priv also take a tag $\tau \in \mathcal{T}$ as input. Accordingly, perfect correctness requires $\mathsf{Pub}(pk_\rho, x, w, \tau) = \Lambda_{sk}(x, \tau) = \mathsf{Priv}(sk, x, \tau)$ for all tags $\tau \in \mathcal{T}$. The formal definition of tag-based QAHPS is shown below.

Definition 12 (Tag-Based QAHPS). *A tag-based QAHPS scheme* $\mathsf{QAHPS} = (\mathsf{Setup}, \alpha_{(\cdot)}, \mathsf{Pub}, \mathsf{Priv})$ *for a language distribution* $\mathscr{L}$ *consists of a tuple of PPT algorithms:*

- $pp \leftarrow_{\$} \mathsf{Setup}(1^\lambda)$*: The setup algorithm outputs a public parameter pp, which implicitly defines* $(\mathcal{SK}, \mathcal{T}, \Pi, \Lambda_{(\cdot)})$*, where*
  - $\mathcal{SK}$ *is the hashing key space,* $\mathcal{T}$ *the tag space and* Π *the hash value space;*
  - $\Lambda_{(\cdot)} : \mathcal{X} \times \mathcal{T} \longrightarrow \Pi$ *is a family of hash functions indexed by a hashing key* $sk \in \mathcal{SK}$*, where* $\mathcal{X}$ *is the universe for languages output by* $\mathscr{L}$*.*

  We assume that $\Lambda_{(\cdot)}$ *is efficiently computable and there are PPT algorithms for sampling* $sk \leftarrow_{\$} \mathcal{SK}$ *uniformly and sampling* $\pi \leftarrow_{\$} \Pi$ *uniformly. We require pp to be an implicit input of other algorithms.*
- $pk_\rho \leftarrow \alpha_\rho(sk)$*: The projection algorithm outputs a projection key* pk_ρ *of hashing key* $sk \in \mathcal{SK}$ *w.r.t. the language parameter* ρ*.*
- $\pi \leftarrow \mathsf{Pub}(pk_\rho, x, w, \tau)$*: The public evaluation algorithm outputs the hash value* $\pi = \Lambda_{sk}(x, \tau) \in \Pi$ *of* $x \in \mathcal{L}_\rho$ *and* $\tau \in \mathcal{T}$*, with the help of the projection key* $pk_\rho = \alpha_\rho(sk)$ *specified by* ρ *and a witness* w *for* $x \in \mathcal{L}_\rho$*.*
- $\pi \leftarrow \mathsf{Priv}(sk, x, \tau)$*: The private evaluation algorithm outputs the hash value* $\pi = \Lambda_{sk}(x, \tau) \in \Pi$ *of* $x \in \mathcal{X}$ *and* $\tau \in \mathcal{T}$*, directly using the hashing key sk.*

Perfect correctness of tag-based QAHPS *requires that, for all possible* $pp \leftarrow_{\$} \mathsf{Setup}(1^\lambda)$ *and* $(\rho, td) \leftarrow_{\$} \mathscr{L}$*, all hashing keys* $sk \in \mathcal{SK}$ *with* $pk_\rho = \alpha_\rho(sk)$ *the corresponding projection key w.r.t.* ρ*, all* $x \in \mathcal{L}_\rho$ *with all possible witnesses* w*, and all tags* $\tau \in \mathcal{T}$*, it holds that*

$$\mathsf{Pub}(pk_\rho, x, w, \tau) \;=\; \Lambda_{sk}(x, \tau) \;=\; \mathsf{Priv}(sk, x, \tau).$$

The notion of LR-ardency is naturally adapted for tag-based QAHPS. A tag-based QAHPS is κ-leakage-resilient $\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-ardent ($\kappa$-LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-ardent), if it is both κ-LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-universal and κ-LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-key-switching.

- **(κ-LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-Universal for Tag-Based QAHPS).** It takes tags into account and considers two hash values with different tags. With overwhelming probability $1 - 2^{-\Omega(\lambda)}$ over $pp \leftarrow_{\$} \mathsf{Setup}(1^\lambda)$, $(\rho_0, td_0) \leftarrow_{\$} \mathscr{L}_0$ and $(\rho_1, td_1) \leftarrow_{\$} \mathscr{L}_1$, for all $x \in \mathcal{X} \setminus (\mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1})$, all $x' \in \mathcal{X}$, all $\tau, \tau' \in \mathcal{T}$ with $\tau \neq \tau'$and all leakage functions $L : \mathcal{SK} \longrightarrow \{0,1\}^\kappa$, if $sk \leftarrow_{\$} \mathcal{SK}$, then

$$\widetilde{\mathbf{H}}_\infty\big(\Lambda_{sk}(x, \tau) \;\big|\; \alpha_{\rho_0}(sk),\ \alpha_{\rho_1}(sk),\ \Lambda_{sk}(x', \tau'),\ L(sk)\big) \;\geq\; \Omega(\lambda).$$

  We require the inequality to hold for adaptive choices of x, x', τ, τ' and L, where they can arbitrarily depend on ρ_0, ρ_1, $\alpha_{\rho_0}(sk)$, $\alpha_{\rho_1}(sk)$.
- **(κ-LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-Key-Switching for Tag-Based QAHPS).** This property remains the same as (9) for the non-tag-based QAHPS, since no tag is involved in the projection algorithm $\alpha_{(\cdot)}$.

Similarly, the κ-LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-weak-ardency of tag-based QAHPS asks for both $\langle \perp, \perp \rangle$-universal and κ-LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-key-switching properties.

- **($\langle\perp,\perp\rangle$-Universal for Tag-Based QAHPS).** With overwhelming probability $1-2^{-\Omega(\lambda)}$ over $pp \leftarrow_{\$} \mathsf{Setup}(1^\lambda)$, for all $x, x' \in \mathcal{X}$, all $\tau, \tau' \in \mathcal{T}$ with $\tau \neq \tau'$ and all leakage functions $L : \mathcal{SK} \longrightarrow \{0,1\}^\kappa$, it holds that:
$$\widetilde{\mathbf{H}}_\infty\big(\Lambda_{sk}(x,\tau) \bigm| \Lambda_{sk}(x',\tau')\big) \ \geq\ \Omega(\lambda),$$
where the probability is over $sk \leftarrow_{\$} \mathcal{SK}$ and x, τ can arbitrarily depend on $\Lambda_{sk}(x',\tau')$.

We also give a game-based definition for LR-ardency of tag-based QAHPS in Appendix C.

4 LR-CCA-Secure PKE via LR-Ardent QAHPS

We present a modular approach to tightly LR-CCA secure PKE from LR-ardent QAHPS. Our approach employs an LR-weak-ardent QAHPS, an LR-ardent $\widehat{\mathsf{QAHPS}}$ and an LR-weak-ardent tag-based $\widetilde{\mathsf{QAHPS}}$, all of which are associated with the same language distribution $\mathscr{L}$.

4.1 The Generic Construction of PKE

Our PKE construction makes use of the following building blocks.

- Three language distributions $\mathscr{L}, \mathscr{L}_0$ and $\mathscr{L}_1$, all of which have hard subset membership problems.
- An LR-weak-ardent $\mathsf{QAHPS} = (\mathsf{Setup}, \alpha_{(\cdot)}, \mathsf{Pub}, \mathsf{Priv})$ for $\mathscr{L}$, whose hash value space Π is an (additive) group.
- An LR-ardent $\widehat{\mathsf{QAHPS}} = (\widehat{\mathsf{Setup}}, \widehat{\alpha}_{(\cdot)}, \widehat{\mathsf{Pub}}, \widehat{\mathsf{Priv}})$ for $\mathscr{L}$.
- An LR-weak-ardent tag-based $\widetilde{\mathsf{QAHPS}} = (\widetilde{\mathsf{Setup}}, \widetilde{\alpha}_{(\cdot)}, \widetilde{\mathsf{Pub}}, \widetilde{\mathsf{Priv}})$ for $\mathscr{L}$, whose tag space is $\widetilde{\mathcal{T}}$.
- A collision-resistant function family $\mathcal{H} = \{\mathsf{H} : \mathcal{X} \times \Pi \longrightarrow \widetilde{\mathcal{T}}\}$.

The LR-ardency requirements for the QAHPS schemes are listed in Table 2.

Table 2. Requirements on QAHPS, $\widehat{\mathsf{QAHPS}}$ and tag-based $\widetilde{\mathsf{QAHPS}}$ for κ-LR-CCA security of PKE. Here $\langle\mathscr{L}_0,\mathscr{L}_1\rangle$-key-switching for $\widehat{\mathsf{QAHPS}}$ is not listed, since it is not necessary in the κ-LR-CCA security proof. We stress that the $\langle\perp,\perp\rangle$-universal property of QAHPS, the $\langle\mathscr{L}_0,\mathscr{L}_1\rangle$-universal property of $\widehat{\mathsf{QAHPS}}$, and the $\langle\perp,\perp\rangle$-universal and $\langle\mathscr{L}_0,\mathscr{L}_1\rangle$-key-switching properties of $\widetilde{\mathsf{QAHPS}}$ do not have to be leakage-resilient.

	LR-weak-ardency of QAHPS	LR-ardency of $\widehat{\mathsf{QAHPS}}$	LR-weak-ardency of $\widetilde{\mathsf{QAHPS}}$
universal	$\langle\perp,\perp\rangle$	κ-LR-$\langle\mathscr{L},\mathscr{L}_0\rangle$, $\langle\mathscr{L}_0,\mathscr{L}_1\rangle$	$\langle\perp,\perp\rangle$
key-switching	κ-LR-$\langle\mathscr{L},\mathscr{L}_0\rangle$	κ-LR-$\langle\mathscr{L},\mathscr{L}_0\rangle$	κ-LR-$\langle\mathscr{L},\mathscr{L}_0\rangle$, $\langle\mathscr{L}_0,\mathscr{L}_1\rangle$

The proposed scheme $\mathsf{PKE} = (\mathsf{Param}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M} = \Pi$ is presented in Fig. 2. The perfect correctness of PKE follows from the perfect correctness of QAHPS, $\widehat{\mathsf{QAHPS}}$ and $\widetilde{\mathsf{QAHPS}}$ directly.

Remark 8 (A More Efficient Variant). If $\widehat{\mathsf{QAHPS}}$ and tag-based $\widetilde{\mathsf{QAHPS}}$ share the same hash value space (i.e., $\widehat{\Pi} = \widetilde{\Pi}$) and $\widehat{\Pi}$ $(= \widetilde{\Pi})$ is an (additive) group[7], the hash values $\widehat{\pi}$ and $\widetilde{\pi}$ can be combined into $\widehat{\pi} + \widetilde{\pi}$, thus saving one element from the ciphertext. This more efficient variant of generic PKE construction is shown in Fig. 15 in Appendix D.

[7] In fact, this condition can be weakened by only requiring $\widehat{\Pi}$ and $\widetilde{\Pi}$ to be subsets of an (additive) group.

$\underline{\mathsf{PP} \leftarrow_{\$} \mathsf{Param}(1^\lambda)\text{:}}$

$pp \leftarrow_{\$} \mathsf{Setup}(1^\lambda)$, which defines $(\mathcal{SK}, \Pi, \Lambda_{(\cdot)})$.

$\widehat{pp} \leftarrow_{\$} \widehat{\mathsf{Setup}}(1^\lambda)$, which defines $(\widehat{\mathcal{SK}}, \widehat{\Pi}, \widehat{\Lambda}_{(\cdot)})$.

$\widetilde{pp} \leftarrow_{\$} \widetilde{\mathsf{Setup}}(1^\lambda)$, which defines $(\widetilde{\mathcal{SK}}, \widetilde{\mathcal{T}}, \widetilde{\Pi}, \widetilde{\Lambda}_{(\cdot)})$.

$(\rho, td) \leftarrow_{\$} \mathscr{L}$. $\quad \mathsf{H} \leftarrow_{\$} \mathcal{H}$.

$\Rightarrow \mathsf{PP} := (pp, \widehat{pp}, \widetilde{pp}, \rho, \mathsf{H})$.

$\underline{C \leftarrow_{\$} \mathsf{Enc}(\mathsf{PK}, M)\text{:}}$

$x \leftarrow_{\$} \mathcal{L}_\rho$ with witness w.

$d := \mathsf{Pub}(pk_\rho, x, w) + M \in \Pi$.

$\tau := \mathsf{H}(x, d) \in \widetilde{\mathcal{T}}$.

$\widehat{\pi} := \widehat{\mathsf{Pub}}(\widehat{pk}_\rho, x, w) \in \widehat{\Pi}$.

$\widetilde{\pi} := \widetilde{\mathsf{Pub}}(\widetilde{pk}_\rho, x, w, \tau) \in \widetilde{\Pi}$.

$\Rightarrow C := (x, d, \widehat{\pi}, \widetilde{\pi})$.

$\underline{(\mathsf{PK}, \mathsf{SK}) \leftarrow_{\$} \mathsf{Gen}(\mathsf{PP})\text{:}}$

$sk \leftarrow_{\$} \mathcal{SK}$. $\quad pk_\rho := \alpha_\rho(sk)$.

$\widehat{sk} \leftarrow_{\$} \widehat{\mathcal{SK}}$. $\quad \widehat{pk}_\rho := \widehat{\alpha}_\rho(\widehat{sk})$.

$\widetilde{sk} \leftarrow_{\$} \widetilde{\mathcal{SK}}$. $\quad \widetilde{pk}_\rho := \widetilde{\alpha}_\rho(\widetilde{sk})$.

$\Rightarrow \mathsf{PK} := (pk_\rho, \widehat{pk}_\rho, \widetilde{pk}_\rho)$,
$\mathsf{SK} := (sk, \widehat{sk}, \widetilde{sk})$.

$\underline{M / \bot \leftarrow \mathsf{Dec}(\mathsf{SK}, C)\text{:}}$

Parse $C = (x, d, \widehat{\pi}', \widetilde{\pi}')$.

$M := d - \mathsf{Priv}(sk, x) \in \Pi$.

$\tau := \mathsf{H}(x, d) \in \widetilde{\mathcal{T}}$.

$\widehat{\pi} := \widehat{\mathsf{Priv}}(\widehat{sk}, x) \in \widehat{\Pi}$.

$\widetilde{\pi} := \widetilde{\mathsf{Priv}}(\widetilde{sk}, x, \tau) \in \widetilde{\Pi}$.

$\Rightarrow$ If $\widehat{\pi}' = \widehat{\pi}$ and $\widetilde{\pi}' = \widetilde{\pi}$, Return M;
Else, Return $\bot$.

Fig. 2. Generic construction of PKE from QAHPS, $\widehat{\mathsf{QAHPS}}$ and tag-based $\widetilde{\mathsf{QAHPS}}$.

4.2 LR-CCA Security of PKE

In this subsection, we prove the LR-CCA security of our generic PKE construction in Fig. 2. The security proof and the concrete security bound also apply to the more efficient variant PKE as shown in Fig. 15 (see Remark 8).

Theorem 1 (LR-CCA Security of PKE). *If (i) $\mathscr{L}$, $\mathscr{L}_0$ and $\mathscr{L}_1$ have hard subset membership problems, (ii)* QAHPS *is a κ-LR-weak-ardent QAHPS scheme for $\mathscr{L}$,* $\widehat{\mathsf{QAHPS}}$ *is a κ-LR-ardent QAHPS scheme for $\mathscr{L}$ and* $\widetilde{\mathsf{QAHPS}}$ *is a κ-LR-weak-ardent tag-based QAHPS scheme for $\mathscr{L}$, which satisfy the properties listed in Table 2, (iii)* QAHPS *is $\mathscr{L}_0$-multi-extracting, (iv) $\mathcal{H}$ is a collision-resistant function family, then the proposed* PKE *scheme in Fig. 2 is κ-LR-CCA secure.*

Concretely, for any adversary $\mathcal{A}$ who makes at most Q_e times of Enc *queries and Q_d times of* Dec *queries, there exist adversaries $\mathcal{B}_1, \cdots, \mathcal{B}_5$, such that $\mathbf{T}(\mathcal{B}_1) \approx \mathbf{T}(\mathcal{B}_4) \approx \mathbf{T}(\mathcal{B}_5) \approx \mathbf{T}(\mathcal{A}) + (Q_e + Q_d) \cdot \mathsf{poly}(\lambda)$, $\mathbf{T}(\mathcal{B}_2) \approx \mathbf{T}(\mathcal{B}_3) \approx \mathbf{T}(\mathcal{A}) + (Q_e + Q_e \cdot Q_d) \cdot \mathsf{poly}(\lambda)$, with $\mathsf{poly}(\lambda)$ independent of $\mathbf{T}(\mathcal{A})$, and*

$$\begin{aligned}\mathsf{Adv}^{\kappa\text{-}lr\text{-}cca}_{\mathsf{PKE},\mathcal{A}}(\lambda) \le\ & \mathsf{Adv}^{Q_e\text{-}msmp}_{\mathscr{L},\mathcal{B}_1}(\lambda) + (2n+1) \cdot \mathsf{Adv}^{Q_e\text{-}msmp}_{\mathscr{L}_0,\mathcal{B}_2}(\lambda) + 2n \cdot \mathsf{Adv}^{Q_e\text{-}msmp}_{\mathscr{L}_1,\mathcal{B}_3}(\lambda) \\ & + \mathsf{Adv}^{cr}_{\mathcal{H},\mathcal{B}_4}(\lambda) + \mathsf{Adv}^{Q_e\text{-}\mathscr{L}_0\text{-}mext}_{\mathsf{QAHPS},\mathcal{B}_5}(\lambda) \\ & + (3 + Q_d + Q_d Q_e + n(Q_d + Q_e + Q_d Q_e)) \cdot 2^{-\Omega(\lambda)}, \text{ for } n = \lceil \log Q_e \rceil.\end{aligned}$$

Remark 9. The last term $(\dots) \cdot 2^{-\Omega(\lambda)}$ in the above security bound encompasses the statistical differences introduced by the universal and key-switching properties of the three QAHPS schemes. We stress that only factors of computational reductions matter to the tightness of a security reduction.

Proof of Theorem 1. We prove the theorem by defining a sequence of games G_0–G_6 and showing adjacent games indistinguishable. (We also illustrate the games in Fig. 16 in Appendix E.) A brief description of differences between adjacent games is summarized in Table 3.

Game G_0: This is the κ-lr-cca security game (cf. Fig. 1). Let Win denote the event that $\beta' = \beta$. By definition, $\mathsf{Adv}^{\kappa\text{-}lr\text{-}cca}_{\mathsf{PKE},\mathcal{A}}(\lambda) = \left|\Pr_0[\mathsf{Win}] - \frac{1}{2}\right|$.

In this game, when answering an Enc query (M_0, M_1), the challenger samples $x^* \leftarrow_{\$} \mathcal{L}_\rho$ with witness w^*, computes $d^* := \mathsf{Pub}(pk_\rho, x^*, w^*) + M_\beta \in \Pi$, $\tau^* := \mathsf{H}(x^*, d^*) \in \widetilde{\mathcal{T}}$, $\widehat{\pi}^* := \widehat{\mathsf{Pub}}(\widehat{pk}_\rho, x^*, w^*) \in \widehat{\Pi}$ and $\widetilde{\pi}^* := \widetilde{\mathsf{Pub}}(\widetilde{pk}_\rho, x^*, w^*, \tau^*) \in \widetilde{\Pi}$. Then, the challenger returns the challenge ciphertext $C^* =$

Table 3. Brief Description of Games G_0–G_6 for the κ-LR-CCA security proof of PKE. Here column "Enc" suggests how the challenge ciphertext $C^* = (x^*, d^*, \widehat{\pi}^*, \widetilde{\pi}^*)$ is generated: sub-column "x^* from" refers to the language from which x^* is chosen; sub-column "d^* using" (resp. "$\widehat{\pi}^*$ using", "$\widetilde{\pi}^*$ using") indicates the keys that are used in the computation of d^* (resp. $\widehat{\pi}^*$, $\widetilde{\pi}^*$). Column "Dec checks" describes the additional check made by Dec upon a decryption query $C = (x, d, \widehat{\pi}', \widetilde{\pi}')$, besides the routine check $C \notin \mathcal{Q}_{\mathcal{ENC}} \wedge \widehat{\pi}' = \widehat{\pi} \wedge \widetilde{\pi}' = \widetilde{\pi}$; Dec outputs $\perp$ if the check fails.

	Enc				Dec checks	Remark/Assumption
	x^* from	d^* using	$\widehat{\pi}^*$ using	$\widetilde{\pi}^*$ using		
G_0	$\mathcal{L}_\rho$	pk_ρ	$\widehat{pk}_\rho$	$\widetilde{pk}_\rho$		κ-LR-CCA game
G_1	$\mathcal{L}_\rho$	sk	$\widehat{sk}$	$\widetilde{sk}$		perfect correctness of QAHPS, $\widehat{\mathsf{QAHPS}}$, $\widetilde{\mathsf{QAHPS}}$
G_2	$\mathcal{L}_\rho$	sk	$\widehat{sk}$	$\widetilde{sk}$	$\tau \notin \mathcal{Q}_{\mathcal{TAG}}$	collision-resistance of $\mathcal{H}$
G_3	$\mathcal{L}_{\rho_0}$	sk	$\widehat{sk}$	$\widetilde{sk}$	$\tau \notin \mathcal{Q}_{\mathcal{TAG}}$	multi-fold SMP of $\mathscr{L}$ and $\mathscr{L}_0$
G_4	$\mathcal{L}_{\rho_0}$	sk	$\widehat{sk}$	$\widetilde{sk}$	$\tau \notin \mathcal{Q}_{\mathcal{TAG}}, x \in \mathcal{L}_\rho$	Lemma 8 (Rejection Lemma) see Table 4 and Table 5
G_5	$\mathcal{L}_{\rho_0}$	sk'	$\widehat{sk}$	$\widetilde{sk}$	$\tau \notin \mathcal{Q}_{\mathcal{TAG}}, x \in \mathcal{L}_\rho$	LR-$\langle \mathscr{L}, \mathscr{L}_0 \rangle$-key-switching of QAHPS
G_6	$\mathcal{L}_{\rho_0}$	$= \mathsf{rand}$	$\widehat{sk}$	$\widetilde{sk}$	$\tau \notin \mathcal{Q}_{\mathcal{TAG}}, x \in \mathcal{L}_\rho$	$\mathscr{L}_0$-multi-extracting of QAHPS

$(x^*, d^*, \widehat{\pi}^*, \widetilde{\pi}^*)$ to the adversary $\mathcal{A}$ and puts C^* to a set $\mathcal{Q}_{\mathcal{ENC}}$. Upon a Dec query $C = (x, d, \widehat{\pi}', \widetilde{\pi}')$, the challenger answers $\mathcal{A}$ as follows. Compute $M := d - \mathsf{Priv}(sk, x) \in \Pi$, $\tau := \mathsf{H}(x, d) \in \widetilde{\mathcal{T}}$, $\widehat{\pi} := \widehat{\mathsf{Priv}}(\widehat{sk}, x) \in \widehat{\Pi}$ and $\widetilde{\pi} := \widetilde{\mathsf{Priv}}(\widetilde{sk}, x, \tau) \in \widetilde{\Pi}$. If $C \notin \mathcal{Q}_{\mathcal{ENC}} \ \wedge\ \widehat{\pi}' = \widehat{\pi} \ \wedge\ \widetilde{\pi}' = \widetilde{\pi}$, return M; otherwise return $\perp$.

Game G_1: It is the same as G_0, except that, when answering $\text{Enc}(M_0, M_1)$, the challenger computes d^*, $\widehat{\pi}^*$ and $\widetilde{\pi}^*$ directly using the secret key $\mathsf{SK} = (sk, \widehat{sk}, \widetilde{sk})$:

- $d^* := \mathsf{Priv}(sk, x^*) + M_\beta \in \Pi$,
- $\widehat{\pi}^* := \widehat{\mathsf{Priv}}(\widehat{sk}, x^*) \in \widehat{\Pi}$ and $\widetilde{\pi}^* := \widetilde{\mathsf{Priv}}(\widetilde{sk}, x^*, \tau^*) \in \widetilde{\Pi}$.

Since $x^* \in \mathcal{L}_\rho$ with witness w^*, by the perfect correctness of QAHPS, $\widehat{\mathsf{QAHPS}}$ and $\widehat{\mathsf{QAHPS}}$, the changes are just conceptual. Consequently, $\Pr_0[\mathsf{Win}] = \Pr_1[\mathsf{Win}]$.

Game G_2: It is the same as G_1, except that, when answering $\text{Enc}(M_0, M_1)$, the challenger also puts τ^* to a set $\mathcal{Q}_{\mathcal{TAG}}$, and when answering $\text{Dec}\big(C = (x, d, \widehat{\pi}', \widetilde{\pi}')\big)$, the challenger adds the following new rejection rule:

- If $\tau \in \mathcal{Q}_{\mathcal{TAG}}$, return $\perp$ directly.

Claim 1. $\big|\Pr_1[\mathsf{Win}] - \Pr_2[\mathsf{Win}]\big| \leq \mathsf{Adv}^{cr}_{\mathcal{H}}(\lambda)$.

Proof. By Coll denote the event that $\mathcal{A}$ ever queries $\text{Dec}\big(C = (x, d, \widehat{\pi}', \widetilde{\pi}')\big)$ s.t.

$$\exists\ C^* = (x^*, d^*, \widehat{\pi}^*, \widetilde{\pi}^*) \in \mathcal{Q}_{\mathcal{ENC}},\ \text{s.t. } C = (x, d, \widehat{\pi}', \widetilde{\pi}') \neq (x^*, d^*, \widehat{\pi}^*, \widetilde{\pi}^*) = C^* \\ \wedge\ \widehat{\pi}' = \widehat{\pi}\ \wedge\ \widetilde{\pi}' = \widetilde{\pi}\ \wedge\ \tau = \mathsf{H}(x, d) = \mathsf{H}(x^*, d^*) = \tau^* \in \mathcal{Q}_{\mathcal{TAG}}.$$

Clearly, G_1 and G_2 are the same until Coll occurs, therefore $\big|\Pr_1[\mathsf{Win}] - \Pr_2[\mathsf{Win}]\big| \leq \Pr_2[\mathsf{Coll}]$. Note that $(x, d) = (x^*, d^*)$ implies $(\widehat{\pi}, \widetilde{\pi}) = (\widehat{\pi}^*, \widetilde{\pi}^*)$. Hence Coll happens if and only if $(x, d) \neq (x^*, d^*)$, which suggests a collision.

Thus, $\big|\Pr_1[\mathsf{Win}] - \Pr_2[\mathsf{Win}]\big| \leq \Pr_2[\mathsf{Coll}] \leq \mathsf{Adv}^{cr}_{\mathcal{H}}(\lambda)$, and Claim 1 follows. ▮

Game G_3: This game is the same as game G_2, except that, in Initialize, the challenger picks $(\rho_0, td_0) \leftarrow_\$ \mathscr{L}_0$ as well, and for all the Enc queries, the challenger samples $x^* \leftarrow_\$ \mathcal{L}_{\rho_0}$ instead of $x^* \leftarrow_\$ \mathcal{L}_\rho$.

Claim 2. $\big|\Pr_2[\mathsf{Win}] - \Pr_3[\mathsf{Win}]\big| \leq \mathsf{Adv}^{Q_e\text{-}msmp}_{\mathscr{L}}(\lambda) + \mathsf{Adv}^{Q_e\text{-}msmp}_{\mathscr{L}_0}(\lambda)$.

Proof. We introduce an intermediate game $\mathsf{G}_{2.5}$ between G_2 and G_3:

– **Game** $\mathsf{G}_{2.5}$**:** It is the same as game G_2, except that $x^* \leftarrow_\$ \mathcal{X}$ in ENC.

Since witness w^* for x^* is not used at all in games G_2, $\mathsf{G}_{2.5}$ and G_3, we can directly construct two adversaries $\mathcal{B}$ and $\mathcal{B}'$ for solving the multi-fold SMP related to $\mathscr{L}$ and the multi-fold SMP related to $\mathscr{L}_0$ respectively, so that $\left|\Pr_2[\mathsf{Win}] - \Pr_{2.5}[\mathsf{Win}]\right| \le \mathsf{Adv}^{Q_e\text{-}msmp}_{\mathscr{L},\mathcal{B}}(\lambda)$ and $\left|\Pr_{2.5}[\mathsf{Win}] - \Pr_3[\mathsf{Win}]\right| \le \mathsf{Adv}^{Q_e\text{-}msmp}_{\mathscr{L}_0,\mathcal{B}'}(\lambda)$. ∎

Game G_4**:** This game is the same as game G_3, except that, when answering $\text{DEC}\big(C = (x, d, \widehat{\pi}', \widetilde{\pi}')\big)$, the challenger adds another new rejection rule:

- If $x \notin \mathcal{L}_\rho$, return $\perp$ directly.

Lemma 8 (Rejection Lemma). *For* $n = \lceil \log Q_e \rceil$, $\left|\Pr_3[\mathsf{Win}] - \Pr_4[\mathsf{Win}]\right| \le 2n \cdot \big(\mathsf{Adv}^{Q_e\text{-}msmp}_{\mathscr{L}_0}(\lambda) + \mathsf{Adv}^{Q_e\text{-}msmp}_{\mathscr{L}_1}(\lambda)\big) + (2 + Q_d + Q_d Q_e + n \cdot (Q_d + Q_e + Q_d Q_e)) \cdot 2^{-\Omega(\lambda)}$.

The proof of Lemma 8 is very modular and relies on the LR-ardency of the three QAHPS schemes. We postpone it to the end of Theorem 1.

Game G_5**:** It is the same as G_4, except that, in INITIALIZE, the challenger picks another $sk' \leftarrow_\$ \mathcal{SK}$ besides sk, and when answering $\text{ENC}(M_0, M_1)$, the challenger computes d^* using sk' rather than sk:

- $d^* := \mathsf{Priv}(sk', x^*) + M_\beta \in \Pi$.

The challenger still uses sk to compute the public key in INITIALIZE and to answer DEC queries.

Claim 3. $|\Pr_4[\mathsf{Win}] - \Pr_5[\mathsf{Win}]| \le 2^{-\Omega(\lambda)}$.

Proof. We analyze the information about sk (resp. sk and sk') that $\mathcal{A}$ may obtain in G_4 (resp. G_5).

- In INITIALIZE, $\mathcal{A}$ obtains $pk_\rho = \alpha_\rho(sk)$ from the public key PK.
- In ENC, since $x^* \leftarrow_\$ \mathcal{L}_{\rho_0}$, the behavior of ENC is completely determined by $\alpha_{\rho_0}(sk)$ (resp. $\alpha_{\rho_0}(sk')$).
- In DEC, the challenger will not output M unless $x \in \mathcal{L}_\rho$ (due to the new rejection rule added in G_4), thus the behavior of DEC is completely determined by $\alpha_\rho(sk)$.
- From oracle $\text{LEAK}(L)$, $\mathcal{A}$ obtains at most κ-bit information of sk.

Note that, L is indeed independent of ρ_0. The reason is as follows: (1) ρ_0 is used only in ENC; (2) $\mathcal{A}$ is not allowed to query LEAK as long as it has queried ENC.

By the κ-LR-$\langle \mathscr{L}, \mathscr{L}_0 \rangle$-key-switching property of QAHPS (cf. (9)), we have

$$\Delta\Big(\ \big(\rho_0,\ \boxed{\alpha_{\rho_0}(sk)}\big)\ ,\ \big(\rho_0,\ \boxed{\alpha_{\rho_0}(sk')}\big)\ \Big|\ \alpha_\rho(sk),\ L(sk)\ \Big)\ \le\ 2^{-\Omega(\lambda)}.$$

Thus, $|\Pr_4[\mathsf{Win}] - \Pr_5[\mathsf{Win}]| \le 2^{-\Omega(\lambda)}$, and Claim 3 follows. ∎

Game G_6**:** This game is the same as game G_5, except that, for all the ENC queries, the challenger samples $d^* \leftarrow_\$ \Pi$ uniformly at random.

Claim 4. $\left|\Pr_5[\mathsf{Win}] - \Pr_6[\mathsf{Win}]\right| \le \mathsf{Adv}^{Q_e\text{-}\mathscr{L}_0\text{-}mext}_{\mathsf{QAHPS}}(\lambda)$.

Proof. The difference between G_5 and G_6 lies in ENC and can be characterized by the following two distributions:

- G_5: $\big(\ x_j^* \leftarrow_\$ \mathcal{L}_{\rho_0},\ d_j^* := \boxed{\mathsf{Priv}(sk', x_j^*)} + M_{\beta,j} \in \Pi\ \big)_{j \in [Q_e]}$,
- G_6: $\big(\ x_j^* \leftarrow_\$ \mathcal{L}_{\rho_0},\ d_j^* \leftarrow_\$ \Pi\ \big)_{j \in [Q_e]}$,

where x_j^*, d_j^*, $M_{\beta,j}$ denote the x^*, d^*, M_β in the j-th Enc query, respectively.

We note that sk' is used only in the computations of d^* in Enc. By the $\mathscr{L}_0$-multi-extracting property of QAHPS, the above two distributions are computationally indistinguishable. Consequently, Claim 4 follows. ▌

Finally in game G_6, d^* is uniformly chosen from Π regardless of the value of β, thus the challenge bit β is completely hidden to $\mathcal{A}$. Then $\Pr_6[\mathsf{Win}] = \frac{1}{2}$. Taking all things together, Theorem 1 follows. □

Proof of Lemma 8 (Rejection Lemma). The difference between game G_3 and game G_4 is the rejection of all ill-formed ciphertexts with $x \notin \mathcal{L}_\rho$ in game G_4. This lemma shows that this rejection rule is undetectable by the adversary $\mathcal{A}$, due to the LR-weak-ardency of QAHPS, the LR-ardency of $\widehat{\mathsf{QAHPS}}$ and the LR-weak-ardency of tag-based $\widetilde{\mathsf{QAHPS}}$. Technically speaking, we modified and adapted the latest partitioning techniques in [GHKP18] (which in turn built upon [GHKW16, Hof17, GHK17]) for our strategy, so that the hash values $\widetilde{\pi} = \widetilde{\Lambda}_{\widetilde{sk}}(x,\tau)$ for $x \notin \mathcal{L}_\rho$ are fully randomized to $\widetilde{\pi} = \widetilde{\Lambda}_{\mathsf{RF}(ctr)}(x,\tau)$ by $\mathsf{RF}(ctr)$, where RF is a random function. This is accomplished in only $O(\log Q_e) = O(\log \lambda)$ steps. Each step is moved forward from $\mathsf{RF}_i(ctr_{|i})$ to $\mathsf{RF}_{i+1}(ctr_{|i+1})$, making use of the LR-universal and LR-key-switching properties of QAHPS, $\widehat{\mathsf{QAHPS}}$ and $\widetilde{\mathsf{QAHPS}}$, together with language switching among $\mathcal{L}_\rho$, $\mathcal{L}_{\rho_0}$ and $\mathcal{L}_{\rho_1}$ (cf. Subsect. 1.1).

Let Bad denote the event that $\mathcal{A}$ ever queries $\textsc{Dec}\big(C = (x, d, \widehat{\pi}', \widetilde{\pi}')\big)$, such that $C \notin \mathcal{Q}_{\mathcal{ENC}} \wedge \widehat{\pi}' = \widehat{\pi} \wedge \widetilde{\pi}' = \widetilde{\pi} \wedge \tau \notin \mathcal{Q}_{\mathcal{TAG}}$ but $x \notin \mathcal{L}_\rho$. Clearly, game G_3 and game G_4 are the same until Bad happens, thus

$$\big|\Pr_3[\mathsf{Win}] - \Pr_4[\mathsf{Win}]\big| \leq \Pr_4[\mathsf{Bad}]. \tag{10}$$

It remains to bound the probability $\Pr_4[\mathsf{Bad}]$. The analysis of this probability is not an easy task. We will defer $\Pr_4[\mathsf{Bad}]$ to a sequence of hybrids H_0–H_4. (We also illustrate the hybrids in Fig. 17 in Appendix E.) A brief description of differences between adjacent hybrids is summarized in Table 4.

Hybrid H_0: It is the same as game G_4. In this hybrid, when answering $\textsc{Dec}\big(C = (x, d, \widehat{\pi}', \widetilde{\pi}')\big)$, the challenger will detect whether or not Bad occurs, and if so, the challenger sets a Boolean variable Bad as true. (As a slight abuse of notation, we use Bad to denote both the event Bad and the Boolean variable Bad.) Therefore, we have

$$\Pr_4[\mathsf{Bad}] = \Pr_{\mathsf{H}0}[\mathsf{Bad}]. \tag{11}$$

Hybrid H_1: It is the same as hybrid H_0, except that, when answering $\textsc{Dec}\big(C = (x, d, \widehat{\pi}', \widetilde{\pi}')\big)$, the challenger adds the following new rule:

- If $x \notin \mathcal{L}_\rho \cup \mathcal{L}_{\rho_0}$, do not check the occurrence of Bad (and return $\perp$ directly).

That is, the challenger will not set the Boolean variable Bad as true unless $x \in \mathcal{L}_{\rho_0}$.

Claim 5. $\big|\Pr_{\mathsf{H}0}[\mathsf{Bad}] - \Pr_{\mathsf{H}1}[\mathsf{Bad}]\big| \leq Q_d \cdot 2^{-\Omega(\lambda)}$.

Proof. Let Forge denote the event that $\mathcal{A}$ ever queries $\textsc{Dec}\big(C = (x, d, \widehat{\pi}', \widetilde{\pi}')\big)$, such that $\widehat{\pi}' = \widehat{\pi}$ but $x \notin \mathcal{L}_\rho \cup \mathcal{L}_{\rho_0}$. Clearly, hybrid H_0 and hybrid H_1 are the same unless Forge happens, thus

$$\big|\Pr_{\mathsf{H}0}[\mathsf{Bad}] - \Pr_{\mathsf{H}1}[\mathsf{Bad}]\big| \leq \Pr_{\mathsf{H}1}[\mathsf{Forge}].$$

We analyze the event Forge in hybrid H_1.

– Observe that the information about $\widehat{sk}$ that $\mathcal{A}$ may obtain in H_1 is only $\widehat{pk}_\rho = \widehat{\alpha}_\rho(\widehat{sk})$ and $\widehat{\alpha}_{\rho_0}(\widehat{sk})$: in Initialize, $\mathcal{A}$ obtains $\widehat{pk}_\rho$ from PK; in Enc, since $x^* \leftarrow_\$ \mathcal{L}_{\rho_0}$, Enc reveals nothing about $\widehat{sk}$ beyond $\widehat{\alpha}_{\rho_0}(\widehat{sk})$; in Dec, the challenger will not output M unless $x \in \mathcal{L}_\rho$ (due to the new rejection rule added in G_4), thus Dec reveals nothing about $\widehat{sk}$ beyond $\widehat{pk}_\rho$; from $\textsc{Leak}(L)$, $\mathcal{A}$ obtains at most κ-bit information of $\widehat{sk}$.

Table 4. Brief Description of Hybrids H_0–H_4 for the κ-LR-CCA security proof of PKE. Here column "Enc (x^* from $\mathcal{L}_{\rho_0}$)" suggests how the challenge ciphertext $C^* = (x^*, d^*, \widehat{\pi}^*, \widetilde{\pi}^*)$ is generated: x^* is always uniformly chosen from $\mathcal{L}_{\rho_0}$; sub-column "$\widehat{\pi}^*$ using" (resp. "$\widetilde{\pi}^*$ using") indicates the keys that are used in the computation of $\widehat{\pi}^*$ (resp. $\widetilde{\pi}^*$). Column "Dec (for $x \notin \mathcal{L}_\rho$)" suggests how a decryption query $C = (x, d, \widehat{\pi}', \widetilde{\pi}')$ with $x \notin \mathcal{L}_\rho$ is handled to check the occurrence of Bad: sub-column "checks" describes the additional check made by Dec besides the routine check $C \notin \mathcal{Q}_{\mathcal{ENC}} \wedge \widehat{\pi}' = \widehat{\pi} \wedge \widetilde{\pi}' = \widetilde{\pi} \wedge \tau \notin \mathcal{Q}_{\mathcal{TAG}}$ ($\mathsf{Bad} := \mathsf{true}$ if the check succeeds); sub-column "$\widehat{\pi}$ using" (resp. "$\widetilde{\pi}$ using") indicates the keys that are used in the computation of $\widehat{\pi}$ (resp. $\widetilde{\pi}$).

	Enc (x^* from $\mathcal{L}_{\rho_0}$)		Dec (for $x \notin \mathcal{L}_\rho$)			Remark/Assumption
	$\widehat{\pi}^*$ using	$\widetilde{\pi}^*$ using	checks	$\widehat{\pi}$ using	$\widetilde{\pi}$ using	
H_0	$\widehat{sk}$	$\widetilde{sk}$		$\widehat{sk}$	$\widetilde{sk}$	$\mathsf{H}_0 = \mathsf{G}_4$
H_1	$\widehat{sk}$	$\widetilde{sk}$	$x \in \mathcal{L}_{\rho_0}$	$\widehat{sk}$	$\widetilde{sk}$	LR-$\langle \mathscr{L}, \mathscr{L}_0 \rangle$-universal of $\widehat{\mathsf{QAHPS}}$
H_2	$\widehat{sk'}$	$\widetilde{sk'}$	$x \in \mathcal{L}_{\rho_0}$	$\widehat{sk'}$	$\widetilde{sk'}$	LR-$\langle \mathscr{L}, \mathscr{L}_0 \rangle$-key-switching of $\widehat{\mathsf{QAHPS}}$, $\widetilde{\mathsf{QAHPS}}$
H_3	$\widehat{sk'}$	$\widetilde{sk'}$		$\widehat{sk'}$	$\widetilde{sk'}$	win. chances increase
$\mathsf{H}_{3.i}$	$\widehat{sk'}$	$\mathsf{RF}_i(ctr_{\vert i})$		$\widehat{sk'}$	$\mathsf{RF}_i(ctr_{\vert i})$ for all $ctr \in [Q_e]$	$\mathsf{H}_3 = \mathsf{H}_{3.0}$ see Table 5
H_4	$\widehat{sk'}$	$\mathsf{RF}_{\lceil \log Q_e \rceil}(ctr)$		$\widehat{sk'}$	$\mathsf{RF}_{\lceil \log Q_e \rceil}(ctr)$ for all $ctr \in [Q_e]$	$\mathsf{H}_4 = \mathsf{H}_{3.\lceil \log Q_e \rceil}$ $\Pr_{\mathsf{H}4}[\mathsf{Bad}] = \mathsf{negl}$: $\langle \bot, \bot \rangle$-universal of $\widetilde{\mathsf{QAHPS}}$

- $ctr \in [Q_e]$ is a counter recording the number of times that the adversary has queried the Enc oracle and is treated as a bit string of length $\lceil \log Q_e \rceil$.
- $\mathsf{RF}_i : \{0,1\}^i \longrightarrow \widetilde{\mathcal{SK}}$ and $\mathsf{RF}_{\lceil \log Q_e \rceil} : \{0,1\}^{\lceil \log Q_e \rceil} \longrightarrow \widetilde{\mathcal{SK}}$ are truly random functions.
- "$\widetilde{\pi}$ using $\mathsf{RF}_i(ctr_{\vert i})$" means $\widetilde{\pi} := \widetilde{\mathsf{Priv}}\big(\mathsf{RF}_i(ctr_{\vert i}), x, \tau\big) \in \widetilde{\Pi}$.
These $\widetilde{\pi}$'s for all $ctr \in [Q_e]$ form a set
$$\mathcal{S} := \big\{ \widetilde{\pi} := \widetilde{\mathsf{Priv}}\big(\mathsf{RF}_i(ctr_{\vert i}), x, \tau\big) \in \widetilde{\Pi} \;\big|\; ctr \in [Q_e] \big\}.$$
- From hybrid $\mathsf{H}_{3.i}$ on, the routine check made by $\text{Dec}\big(C = (x, d, \widehat{\pi}', \widetilde{\pi}')\big)$ for $x \notin \mathcal{L}_\rho$ is
$$C \notin \mathcal{Q}_{\mathcal{ENC}} \;\wedge\; \widehat{\pi}' = \widehat{\pi} \;\wedge\; \widetilde{\pi}' \in \mathcal{S} \;\wedge\; \tau \notin \mathcal{Q}_{\mathcal{TAG}}.$$

– The event Forge occurs in H_1 implies that $\mathcal{A}$ ever makes a Dec query $C = (x, d, \widehat{\pi}', \widetilde{\pi}')$ such that $\widehat{\pi}' = \widehat{\pi}$ but $x \notin \mathcal{L}_\rho \cup \mathcal{L}_{\rho_0}$ hold, where
$$\widehat{\pi} = \widehat{\mathsf{Priv}}(\widehat{sk}, x) = \widehat{\Lambda}_{\widehat{sk}}(x) \in \widehat{\Pi}.$$
Since $\widehat{\mathsf{QAHPS}}$ is κ-$\langle \mathscr{L}, \mathscr{L}_0 \rangle$-universal, $\widehat{\pi}$ has enough entropy even conditioned on $\widehat{pk}_\rho = \widehat{\alpha}_\rho(\widehat{sk})$, $\widehat{\alpha}_{\rho_0}(\widehat{sk})$ and $L(\widehat{sk})$, i.e.
$$\widetilde{\mathbf{H}}_\infty\big(\widehat{\Lambda}_{\widehat{sk}}(x) \;\big|\; \widehat{\alpha}_\rho(\widehat{sk}),\ \widehat{\alpha}_{\rho_0}(\widehat{sk}),\ L(\widehat{sk})\big) \;\geq\; \Omega(\lambda).$$
Consequently, in one Dec query, Forge occurs with probability at most $2^{-\Omega(\lambda)}$.

By a union bound, we get that $\Pr_{\mathsf{H}1}[\mathsf{Forge}] \leq Q_d \cdot 2^{-\Omega(\lambda)}$, thus Claim 5 follows. ▌

Hybrid H_2: This hybrid is the same as hybrid H_1, except that, in Initialize, the challenger picks another pair of $\widehat{sk'} \leftarrow_{\$} \widehat{\mathcal{SK}}$, $\widetilde{sk'} \leftarrow_{\$} \widetilde{\mathcal{SK}}$ besides $\widehat{sk}, \widetilde{sk}$. Moreover, when answering $\text{Enc}(M_0, M_1)$, the challenger computes $\widehat{\pi}^*$, $\widetilde{\pi}^*$ using $\widehat{sk'}$, $\widetilde{sk'}$ rather than $\widehat{sk}$, $\widetilde{sk}$, respectively:

- $\widehat{\pi}^* := \widehat{\mathsf{Priv}}(\widehat{sk'}, x^*) \in \widehat{\Pi}$, $\;\widetilde{\pi}^* := \widetilde{\mathsf{Priv}}(\widetilde{sk'}, x^*, \tau^*) \in \widetilde{\Pi}$.

Furthermore, when answering $\text{DEC}\big(C = (x, d, \widehat{\pi}', \widetilde{\pi}')\big)$, for $x \in \mathcal{L}_{\rho_0}$, the challenger computes $\widehat{\pi}$, $\widetilde{\pi}$ using $\widehat{sk}'$, $\widetilde{sk}'$ (to detect the occurrence of Bad), rather than $\widehat{sk}$, $\widetilde{sk}$, respectively:

- $\widehat{\pi} := \widehat{\mathsf{Priv}}(\widehat{sk}', x) \in \widehat{\Pi}$, $\widetilde{\pi} := \widetilde{\mathsf{Priv}}(\widetilde{sk}', x, \tau) \in \widetilde{\Pi}$.

The challenger still uses $\widehat{sk}, \widetilde{sk}$ to compute the public key in INITIALIZE and to answer DEC queries for $x \in \mathcal{L}_\rho$.

Claim 6. $|\Pr_{\mathsf{H1}}[\mathsf{Bad}] - \Pr_{\mathsf{H2}}[\mathsf{Bad}]| \le 2 \cdot 2^{-\Omega(\lambda)}$.

Proof. We analyze the information about $\widehat{sk}, \widetilde{sk}$ (resp. $\widehat{sk}, \widetilde{sk}$, $\widehat{sk}'$, $\widetilde{sk}'$) that are involved in H_1 (resp. H_2).

- In INITIALIZE, the public key PK contains $\widehat{pk}_\rho = \widehat{\alpha}_\rho(\widehat{sk})$ and $\widetilde{pk}_\rho = \widetilde{\alpha}_\rho(\widetilde{sk})$.
- In ENC, since $x^* \leftarrow_\$ \mathcal{L}_{\rho_0}$, the behavior of ENC is completely determined by $\widehat{\alpha}_{\rho_0}(\widehat{sk})$, $\widetilde{\alpha}_{\rho_0}(\widetilde{sk})$ (resp. $\widehat{\alpha}_{\rho_0}(\widehat{sk}')$, $\widetilde{\alpha}_{\rho_0}(\widetilde{sk}')$).
- In DEC, the challenger will not compute $\widehat{\pi}$ and $\widetilde{\pi}$ unless $x \in \mathcal{L}_\rho \cup \mathcal{L}_{\rho_0}$ (due to the new rule added in H_1), thus: for $x \in \mathcal{L}_\rho$, the behavior of DEC is completely determined by $\widehat{\alpha}_\rho(\widehat{sk})$, $\widetilde{\alpha}_\rho(\widetilde{sk})$; for $x \in \mathcal{L}_{\rho_0}$, the behavior of DEC is completely determined by $\widehat{\alpha}_{\rho_0}(\widehat{sk})$, $\widetilde{\alpha}_{\rho_0}(\widetilde{sk})$ (resp. $\widehat{\alpha}_{\rho_0}(\widehat{sk}')$, $\widetilde{\alpha}_{\rho_0}(\widetilde{sk}')$).
- From LEAK(L), $\mathcal{A}$ obtains at most κ-bit information of $\widehat{sk}$ and $\widetilde{sk}$.

Note that, L is indeed independent of ρ_0. The reason is as follows: (1) The only way that $\mathcal{A}$ learns information about ρ_0 is through oracle ENC (for DEC queries, $\mathcal{A}$ receives $\perp$ immediately if $x \notin \mathcal{L}_\rho$, no matter $x \in \mathcal{L}_{\rho_0}$ or $x \notin \mathcal{L}_\rho \cup \mathcal{L}_{\rho_0}$); (2) $\mathcal{A}$ is not allowed to query oracle LEAK as long as it has queried oracle ENC.

By the κ-LR-$\langle \mathscr{L}, \mathscr{L}_0 \rangle$-key-switching property of $\widehat{\mathsf{QAHPS}}$ and $\widetilde{\mathsf{QAHPS}}$, we have

$$\Delta\Big(\ \big(\rho_0,\ \boxed{\widehat{\alpha}_{\rho_0}(\widehat{sk})}\big)\ ,\ \big(\rho_0,\ \boxed{\widehat{\alpha}_{\rho_0}(\widehat{sk}')}\big)\ \big|\ \widehat{\alpha}_\rho(\widehat{sk}),\ L(\widehat{sk})\ \Big)\ \le\ 2^{-\Omega(\lambda)},$$

$$\Delta\Big(\ \big(\rho_0,\ \boxed{\widetilde{\alpha}_{\rho_0}(\widetilde{sk})}\big)\ ,\ \big(\rho_0,\ \boxed{\widetilde{\alpha}_{\rho_0}(\widetilde{sk}')}\big)\ \big|\ \widetilde{\alpha}_\rho(\widetilde{sk}),\ L(\widetilde{sk})\ \Big)\ \le\ 2^{-\Omega(\lambda)},$$

where $|L(\widehat{sk})| \le \kappa$ and $|L(\widetilde{sk})| \le \kappa$. Consequently, $|\Pr_{\mathsf{H1}}[\mathsf{Bad}] - \Pr_{\mathsf{H2}}[\mathsf{Bad}]| \le 2 \cdot 2^{-\Omega(\lambda)}$, and Claim 6 follows. ∎

Hybrid H_3: This hybrid is the same as hybrid H_2, except that, when answering $\text{DEC}\big(C = (x, d, \widehat{\pi}', \widetilde{\pi}')\big)$, the challenger removes the new rule added in hybrid H_1. In other words,

- If $x \notin \mathcal{L}_\rho$, the challenger detects whether or not Bad occurs no matter $x \in \mathcal{L}_{\rho_0}$ or $x \notin \mathcal{L}_\rho \cup \mathcal{L}_{\rho_0}$.

Note that, with this removal, the trapdoor td_0 for $\mathcal{L}_{\rho_0}$ is not needed any more in hybrid H_3. (Jumping ahead, this serves as a preparation for the language switching in hybrid $\mathsf{H}_{3.i.1}$.)

Obviously, this change can only increase the probability of Bad. Thus, we have $\Pr_{\mathsf{H2}}[\mathsf{Bad}] \le \Pr_{\mathsf{H3}}[\mathsf{Bad}]$.

Hybrid $\mathsf{H}_{3.i}$, $i \in [0, n]$ with $n = \lceil \log Q_e \rceil$: This hybrid is the same as H_3, except that, when answering the ctr-th $\text{ENC}(M_0, M_1)$ query, where $ctr \in [Q_e]$, the challenger computes $\widetilde{\pi}^*$ using $\mathsf{RF}_i(ctr_{|i})$ rather than $\widetilde{sk}'$:

- $\widetilde{\pi}^* := \widetilde{\mathsf{Priv}}\big(\mathsf{RF}_i(ctr_{|i}), x^*, \tau^*\big) \in \widetilde{\Pi}$.

Here $ctr \in [Q_e]$ is a counter recording the serial number of ENC query issued by the adversary and is treated as a bit string of length $n = \lceil \log Q_e \rceil$, $ctr_{|i} \in \{0,1\}^i$ denotes the first i bits of ctr, and $\mathsf{RF}_i : \{0,1\}^i \longrightarrow \widetilde{\mathcal{SK}}$ is a truly random function implemented by the challenger on the fly. Moreover, when answering $\text{DEC}\big(C = (x, d, \widehat{\pi}', \widetilde{\pi}')\big)$, for $x \notin \mathcal{L}_\rho$, the challenger computes a set $\mathcal{S}$ of $\widetilde{\pi}$'s using $\mathsf{RF}_i(ctr_{|i})$ rather than $\widetilde{sk}'$ for all $ctr \in [Q_e]$:

- $\mathcal{S} := \big\{ \widetilde{\pi} := \widetilde{\mathsf{Priv}}\big(\mathsf{RF}_i(ctr_{|i}), x, \tau\big) \in \widetilde{\Pi} \;\big|\; ctr \in [Q_e] \big\}$,

and sets the Boolean variable Bad as true as long as $\widetilde{\pi}' \in \mathcal{S}$ (as well as $C \notin \mathcal{Q}_{\mathcal{ENC}} \wedge \widehat{\pi}' = \widehat{\pi} \wedge (\tau, d) \notin \mathcal{Q}_{\mathcal{TAG}}$ holds).

In hybrid $\mathsf{H}_{3.0}$, the challenger will use $\mathsf{RF}_0(ctr_{|0}) = \mathsf{RF}_0(\varepsilon)$ in ENC and DEC. Since $\mathsf{RF}_0(\varepsilon)$ is a single random element in $\widetilde{\mathcal{SK}}$, the same as $\widetilde{sk}'$, $\mathsf{H}_{3.0}$ is essentially the same as H_3. Consequently, we have $\Pr_{\mathsf{H}3}[\mathsf{Bad}] = \Pr_{\mathsf{H}3.0}[\mathsf{Bad}]$.

Next, we will defer Bad from hybrid $\mathsf{H}_{3.i}$ to $\mathsf{H}_{3.i+1}$, for any $i \in [0, n-1]$. To this end, we introduce a sequence of hybrids $\{\mathsf{H}_{3.i.1}\text{–}\mathsf{H}_{3.i.6}\}_{i\in[0,n-1]}$ in-between. (We also illustrate the intermediate hybrids in Fig. 18 in Appendix E.) A brief description of differences between adjacent hybrids is summarized in Table 5.

Hybrid $\mathsf{H}_{3.i.1}$, $i \in [0, n-1]$: This hybrid is the same as hybrid $\mathsf{H}_{3.i}$, except that, in INITIALIZE, the challenger picks another $(\rho_1, td_1) \leftarrow_{\$} \mathscr{L}_1$ besides $(\rho, td) \leftarrow_{\$} \mathscr{L}$ and $(\rho_0, td_0) \leftarrow_{\$} \mathscr{L}_0$, and for the ctr-th ENC query, where $ctr \in [Q_e]$, the challenger samples $x^* \leftarrow_{\$} \mathcal{L}_{\rho_{ctr_{i+1}}}$ according to the $(i+1)$-th bit of ctr, i.e., $x^* \leftarrow_{\$} \mathcal{L}_{\rho_0}$ if $ctr_{i+1} = 0$ and $x^* \leftarrow_{\$} \mathcal{L}_{\rho_1}$ if $ctr_{i+1} = 1$.

Claim 7. $\big|\Pr_{\mathsf{H}3.i}[\mathsf{Bad}] - \Pr_{\mathsf{H}3.i.1}[\mathsf{Bad}]\big| \le \mathsf{Adv}^{Q_e\text{-}msmp}_{\mathscr{L}_0}(\lambda) + \mathsf{Adv}^{Q_e\text{-}msmp}_{\mathscr{L}_1}(\lambda)$.

Proof. For convenience, we introduce an intermediate hybrid $\mathsf{H}_{3.i.0}$ between $\mathsf{H}_{3.i}$ and $\mathsf{H}_{3.i.1}$:

– **Hybrid $\mathsf{H}_{3.i.0}$:** It is the same as hybrid $\mathsf{H}_{3.i}$, except that, for the ctr-th ENC query, where $ctr \in [Q_e]$, the challenger samples $x^* \leftarrow_{\$} \mathcal{L}_{\rho_0}$ if $ctr_{i+1} = 0$ and $x^* \leftarrow_{\$} \mathcal{X}$ if $ctr_{i+1} = 1$.

Since witness w^* for x^* is not used at all in hybrids $\mathsf{H}_{3.i}$, $\mathsf{H}_{3.i.0}$ and $\mathsf{H}_{3.i.1}$, we can directly construct two adversaries $\mathcal{B}$ and $\mathcal{B}'$ for solving the multi-fold SMP related to $\mathscr{L}_0$ and the multi-fold SMP related to $\mathscr{L}_1$ respectively, such that $\big|\Pr_{\mathsf{H}3.i}[\mathsf{Bad}] - \Pr_{\mathsf{H}3.i.0}[\mathsf{Bad}]\big| \le \mathsf{Adv}^{Q_e\text{-}msmp}_{\mathscr{L}_0,\mathcal{B}}(\lambda)$ and $\big|\Pr_{\mathsf{H}3.i.0}[\mathsf{Bad}] - \Pr_{\mathsf{H}3.i.1}[\mathsf{Bad}]\big| \le \mathsf{Adv}^{Q_e\text{-}msmp}_{\mathscr{L}_1,\mathcal{B}'}(\lambda)$. More precisely, $\mathcal{B}$ and $\mathcal{B}'$ generate $(\rho, td) \leftarrow_{\$} \mathscr{L}$, the secret key $\mathsf{SK} = (sk, \widehat{sk}, \widetilde{sk})$, $\widehat{sk}'$ and implement the random function RF_i themselves, thus they can answer DEC queries perfectly for $\mathcal{A}$ and check the occurrence of Bad (by using td to determine whether or not $x \in \mathcal{L}_\rho$); as for ENC queries, $\mathcal{B}$ and $\mathcal{B}'$ sample $x^* \leftarrow_{\$} \mathcal{L}_{\rho_0}$ honestly if $ctr_{i+1} = 0$ and embed their challenges directly to x^* if $ctr_{i+1} = 1$, then compute d^*, $\widehat{\pi}^*$ and $\widetilde{\pi}^*$ from x^* with the help of sk, $\widehat{sk}'$ and $\mathsf{RF}_i(ctr_{|i})$, without knowing a witness for x^*; finally, $\mathcal{B}$ and $\mathcal{B}'$ output 1 if Bad occurs. Consequently, Claim 7 follows. ∎

Hybrid $\mathsf{H}_{3.i.2}$, $i \in [0, n-1]$: This hybrid is the same as $\mathsf{H}_{3.i.1}$, except that, when answering $\mathrm{DEC}\big(C = (x, d, \widehat{\pi}', \widetilde{\pi}')\big)$, the challenger adds the following new rule:

- If $x \notin \mathcal{L}_\rho \cup \mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1}$, do not check the occurrence of Bad (and return $\perp$ directly).

That is, the challenger will not set the Boolean variable Bad as true unless $x \in \mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1}$.

Claim 8. $\big|\Pr_{\mathsf{H}3.i.1}[\mathsf{Bad}] - \Pr_{\mathsf{H}3.i.2}[\mathsf{Bad}]\big| \le Q_d \cdot 2^{-\Omega(\lambda)}$.

Proof. Let Forge denote the event that $\mathcal{A}$ ever queries $\mathrm{DEC}\big(C = (x, d, \widehat{\pi}', \widetilde{\pi}')\big)$, such that $\widehat{\pi}' = \widehat{\pi}$ but $x \notin \mathcal{L}_\rho \cup \mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1}$. Clearly, hybrid $\mathsf{H}_{3.i.1}$ and hybrid $\mathsf{H}_{3.i.2}$ are the same unless Forge happens, thus

$$\big|\Pr_{\mathsf{H}3.i.1}[\mathsf{Bad}] - \Pr_{\mathsf{H}3.i.2}[\mathsf{Bad}]\big| \le \Pr_{\mathsf{H}3.i.2}[\mathsf{Forge}].$$

We analyze the event Forge in hybrid $\mathsf{H}_{3.i.2}$.

– Observe that the information about $\widehat{sk}'$ that $\mathcal{A}$ may obtain in $\mathsf{H}_{3.i.2}$ is only $\widehat{\alpha}_{\rho_0}(\widehat{sk}')$ and $\widehat{\alpha}_{\rho_1}(\widehat{sk}')$: in INITIALIZE, the computation of PK does not involve $\widehat{sk}'$ (recall that it uses $\widehat{sk}$); in ENC, since $x^* \leftarrow_{\$} \mathcal{L}_{\rho_{ctr_{i+1}}}$ according to the $(i+1)$-th bit of ctr so that $x^* \in \mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1}$, ENC reveals nothing

Table 5. Brief Description of Hybrids $\mathsf{H}_{3.i}$, $\mathsf{H}_{3.i.1}$–$\mathsf{H}_{3.i.6}$, $\mathsf{H}_{3.(i+1)}$ for the κ-LR-CCA security proof of PKE. Here column "Enc" suggests how the challenge ciphertext $C^* = (x^*, d^*, \widehat{\pi}^*, \widetilde{\pi}^*)$ is generated: sub-column "x^* from" refers to the language from which x^* is chosen; sub-column "$\widehat{\pi}^*$ using" (resp. "$\widetilde{\pi}^*$ using") indicates the keys that are used in the computation of $\widehat{\pi}^*$ (resp. $\widetilde{\pi}^*$). Column "Dec (for $x \notin \mathcal{L}_\rho$)" suggests how a decryption query $C = (x, d, \widehat{\pi}', \widetilde{\pi}')$ with $x \notin \mathcal{L}_\rho$ is handled to check the occurrence of Bad: sub-column "checks" describes the additional check made by Dec besides the routine check $C \notin \mathcal{Q}_{\mathcal{ENC}} \wedge \widehat{\pi}' = \widehat{\pi} \wedge \widetilde{\pi}' \in \mathcal{S} \wedge \tau \notin \mathcal{Q}_{\mathcal{TAG}}$ ($\mathsf{Bad} := \mathsf{true}$ if the check succeeds); sub-column "$\widehat{\pi}$ using" (resp. "$\widetilde{\pi}$ using") indicates the keys that are used in the computation of $\widehat{\pi}$ (resp. $\widetilde{\pi}$).

	Enc			Dec (for $x \notin \mathcal{L}_\rho$)			Remark/Assumption
	x^* from	$\widehat{\pi}^*$ using	$\widetilde{\pi}^*$ using	checks	$\widehat{\pi}$ using	$\widetilde{\pi}$ using (for all $ctr \in [Q_e]$)	
$\mathsf{H}_{3.i}$	$\mathcal{L}_{\rho_0}$	$\widehat{sk}'$	$\mathsf{RF}_i(ctr_{\vert i})$		$\widehat{sk}'$	$\mathsf{RF}_i(ctr_{\vert i})$	
$\mathsf{H}_{3.i.1}$	$\mathcal{L}_{\rho_{ctr_{i+1}}}$		$\mathsf{RF}_i(ctr_{\vert i})$			$\mathsf{RF}_i(ctr_{\vert i})$	multi-fold SMP of $\mathscr{L}_0$ and $\mathscr{L}_1$
$\mathsf{H}_{3.i.2}$	$\mathcal{L}_{\rho_{ctr_{i+1}}}$		$\mathsf{RF}_i(ctr_{\vert i})$	$x \in \mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1}$		$\mathsf{RF}_i(ctr_{\vert i})$	$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-universal of $\widehat{\mathsf{QAHPS}}$
$\mathsf{H}_{3.i.3}$	$\mathcal{L}_{\rho_{ctr_{i+1}}}$		$\mathsf{RF}_{i+1}(ctr_{\vert i+1})$	$x \in \mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1}$		$\mathsf{RF}_{i+1}(ctr_{\vert i} \Vert d_x)$	$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-key-switching of $\widetilde{\mathsf{QAHPS}}$
$\mathsf{H}_{3.i.4}$	$\mathcal{L}_{\rho_{ctr_{i+1}}}$		$\mathsf{RF}_{i+1}(ctr_{\vert i+1})$	$x \in \mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1}$		$\mathsf{RF}_{i+1}(ctr_{\vert i} \Vert b)$ for $b \in \{0,1\}$	win. chances increase
$\mathsf{H}_{3.i.5}$	$\mathcal{L}_{\rho_{ctr_{i+1}}}$		$\mathsf{RF}_{i+1}(ctr_{\vert i+1})$	$x \in \mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1}$		$\mathsf{RF}_{i+1}(ctr_{\vert i+1})$	$\langle \bot, \bot \rangle$-universal of $\widetilde{\mathsf{QAHPS}}$
$\mathsf{H}_{3.i.6}$	$\mathcal{L}_{\rho_{ctr_{i+1}}}$		$\mathsf{RF}_{i+1}(ctr_{\vert i+1})$			$\mathsf{RF}_{i+1}(ctr_{\vert i+1})$	win. chances increase
$\mathsf{H}_{3.(i+1)}$	$\mathcal{L}_{\rho_0}$		$\mathsf{RF}_{i+1}(ctr_{\vert i+1})$			$\mathsf{RF}_{i+1}(ctr_{\vert i+1})$	multi-fold SMP of $\mathscr{L}_0$ and $\mathscr{L}_1$

- $\mathsf{RF}_i : \{0,1\}^i \longrightarrow \widetilde{\mathcal{SK}}$ and $\mathsf{RF}_{i+1} : \{0,1\}^{i+1} \longrightarrow \widetilde{\mathcal{SK}}$ are truly random functions.
- For $x \in \mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1}$, $d_x := 0$ if $x \in \mathcal{L}_{\rho_0}$ and $d_x := 1$ if $x \in \mathcal{L}_{\rho_1}$.
- "$\widetilde{\pi}$ using $\mathsf{RF}_i(ctr_{\vert i})$" means $\widetilde{\pi} := \widetilde{\mathsf{Priv}}(\mathsf{RF}_i(ctr_{\vert i}), x, \tau) \in \widetilde{\Pi}$.

  These $\widetilde{\pi}$'s for all $ctr \in [Q_e]$ form a set

$$\mathcal{S} := \{\, \widetilde{\pi} := \widetilde{\mathsf{Priv}}(\mathsf{RF}_i(ctr_{\vert i}), x, \tau) \in \widetilde{\Pi} \mid ctr \in [Q_e] \,\}.$$

about $\widehat{sk}'$ beyond $\widehat{\alpha}_{\rho_0}(\widehat{sk}')$ and $\widehat{\alpha}_{\rho_1}(\widehat{sk}')$; in Dec, the challenger will not output M unless $x \in \mathcal{L}_\rho$, and for $x \in \mathcal{L}_\rho$, the computation of $\widehat{\pi}$ uses $\widehat{sk}$ rather than $\widehat{sk}'$, thus Dec reveals nothing about $\widehat{sk}'$ to $\mathcal{A}$. Note that Leak only leaks information about $\mathsf{SK} = (sk, \widehat{sk}, \widetilde{sk})$ and no information about $\widehat{sk}'$ is leaked to $\mathcal{A}$.

– The event Forge occurs in $\mathsf{H}_{3.i.2}$ implies that $\mathcal{A}$ ever makes a Dec query $C = (x, d, \widehat{\pi}', \widetilde{\pi}')$ such that $\widehat{\pi}' = \widehat{\pi}$ but $x \notin \mathcal{L}_\rho \cup \mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1}$ hold, where

$$\widehat{\pi} = \widehat{\mathsf{Priv}}(\widehat{sk}', x) = \widehat{\Lambda}_{\widehat{sk}'}(x) \in \widehat{\Pi}.$$

Since $\widehat{\mathsf{QAHPS}}$ is $\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-universal, $\widehat{\pi}$ has enough entropy conditioned on $\widehat{\alpha}_{\rho_0}(\widehat{sk}')$ and $\widehat{\alpha}_{\rho_1}(\widehat{sk}')$, i.e.,

$$\widetilde{\mathbf{H}}_\infty\big(\widehat{\Lambda}_{\widehat{sk}'}(x) \bigm| \widehat{\alpha}_{\rho_0}(\widehat{sk}'),\ \widehat{\alpha}_{\rho_1}(\widehat{sk}')\big) \ \geq\ \Omega(\lambda).$$

Consequently, in one Dec query, Forge occurs with probability at most $2^{-\Omega(\lambda)}$.

By a union bound, $\Pr_{\mathsf{H}3.i.2}[\mathsf{Forge}] \leq Q_d \cdot 2^{-\Omega(\lambda)}$, thus Claim 8 follows. ▌

Hybrid $\mathsf{H}_{3.i.3}$, $i \in [0, n-1]$: This hybrid is the same as hybrid $\mathsf{H}_{3.i.2}$, except that, when answering the ctr-th Enc query, where $ctr \in [Q_e]$, the challenger computes $\widetilde{\pi}^*$ using $\mathsf{RF}_{i+1}(ctr_{\vert i+1})$ rather than $\mathsf{RF}_i(ctr_{\vert i})$:

- $\widetilde{\pi}^* := \widetilde{\mathsf{Priv}}\big(\mathsf{RF}_{i+1}(ctr_{|i+1}), x^*, \tau^*\big) \in \widetilde{\Pi}$.

Moreover, when answering $\textsc{Dec}\big(C = (x, d, \widehat{\pi}', \widetilde{\pi}')\big)$, for $x \in \mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1}$, the challenger computes the set $\mathcal{S}$ using $\mathsf{RF}_{i+1}(ctr_{|i}||d_x)$ rather than $\mathsf{RF}_i(ctr_{|i})$:

- $\mathcal{S} := \big\{ \widetilde{\pi} := \widetilde{\mathsf{Priv}}\big(\mathsf{RF}_{i+1}(ctr_{|i}||d_x), x, \tau\big) \in \widetilde{\Pi} \;\big|\; ctr \in [Q_e] \big\}$.

Here $d_x \in \{0,1\}$ is defined as

$$d_x := \begin{cases} 0, & \text{if } x \in \mathcal{L}_{\rho_0} \\ 1, & \text{if } x \in \mathcal{L}_{\rho_1} \end{cases},$$

and $\mathsf{RF}_{i+1} : \{0,1\}^{i+1} \longrightarrow \widetilde{\mathcal{SK}}$ is a truly random function implemented by the challenger on the fly. For the convenience of our analysis, we assume that RF_{i+1} is implemented via

$$\mathsf{RF}_{i+1}(ctr_{|i}||b) := \begin{cases} \mathsf{RF}_i(ctr_{|i}), & \text{if } b = 0 \\ \overline{\mathsf{RF}}_i(ctr_{|i}), & \text{if } b = 1 \end{cases},$$

where $\overline{\mathsf{RF}}_i : \{0,1\}^i \longrightarrow \widetilde{\mathcal{SK}}$ is an independent random function.

Claim 9. $\big|\Pr_{\mathsf{H}3.i.2}[\mathsf{Bad}] - \Pr_{\mathsf{H}3.i.3}[\mathsf{Bad}]\big| \leq Q_e \cdot 2^{-\Omega(\lambda)}$.

Proof. We analyze the information about $\mathsf{RF}_i(ctr_{|i})$ (resp. $\mathsf{RF}_i(ctr_{|i})$ and $\overline{\mathsf{RF}}_i(ctr_{|i})$) that are involved in $\mathsf{H}_{3.i.2}$ (resp. $\mathsf{H}_{3.i.3}$).

- In $\textsc{Enc}$, $x^* \leftarrow_\$ \mathcal{L}_{\rho_{ctr_{i+1}}}$ according to the $(i+1)$-th bit of ctr:
  - if $ctr_{i+1} = 0$, then $x^* \in \mathcal{L}_{\rho_0}$, thus the behavior of $\textsc{Enc}$ is completely determined by $\widetilde{\alpha}_{\rho_0}(\mathsf{RF}_i(ctr_{|i}))$ (resp. $\widetilde{\alpha}_{\rho_0}(\mathsf{RF}_{i+1}(ctr_{|i+1})) = \widetilde{\alpha}_{\rho_0}(\mathsf{RF}_i(ctr_{|i}))$);
  - if $ctr_{i+1} = 1$, then $x^* \in \mathcal{L}_{\rho_1}$, thus the behavior of $\textsc{Enc}$ is completely determined by $\widetilde{\alpha}_{\rho_1}(\mathsf{RF}_i(ctr_{|i}))$ (resp. $\widetilde{\alpha}_{\rho_1}(\mathsf{RF}_{i+1}(ctr_{|i+1})) = \widetilde{\alpha}_{\rho_1}(\overline{\mathsf{RF}}_i(ctr_{|i}))$).
- In $\textsc{Dec}$, the challenger will not compute $\widetilde{\pi}$ unless $x \in \mathcal{L}_\rho \cup \mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1}$ (due to the new rule added in $\mathsf{H}_{3.i.2}$):
  - for $x \in \mathcal{L}_\rho$, $\widetilde{\pi}$ is computed using $\widetilde{sk}$, neither $\mathsf{RF}_i(ctr_{|i})$ nor $\overline{\mathsf{RF}}_i(ctr_{|i})$ is involved;
  - for $x \in \mathcal{L}_{\rho_0}$, $d_x = 0$, thus the behavior of $\textsc{Dec}$ is completely determined by $\widetilde{\alpha}_{\rho_0}(\mathsf{RF}_i(ctr_{|i}))$ (resp. $\widetilde{\alpha}_{\rho_0}(\mathsf{RF}_{i+1}(ctr_{|i}||d_x)) = \widetilde{\alpha}_{\rho_0}(\mathsf{RF}_i(ctr_{|i}))$);
  - for $x \in \mathcal{L}_{\rho_1}$, $d_x = 1$, thus the behavior of $\textsc{Dec}$ is completely determined by $\widetilde{\alpha}_{\rho_1}(\mathsf{RF}_i(ctr_{|i}))$ (resp. $\widetilde{\alpha}_{\rho_1}(\mathsf{RF}_{i+1}(ctr_{|i}||d_x)) = \widetilde{\alpha}_{\rho_1}(\overline{\mathsf{RF}}_i(ctr_{|i}))$).
- $\textsc{Leak}$ only leaks information about $\mathsf{SK} = (sk, \widehat{sk}, \widetilde{sk})$ and no information about $\mathsf{RF}_i(ctr_{|i})$ is leaked to $\mathcal{A}$.

By the $\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-key-switching property of $\widetilde{\mathsf{QAHPS}}$, for any $ctr \in [Q_e]$, we have

$$\Delta\Big(\big(\rho_1,\ \widetilde{\alpha}_{\rho_1}(\mathsf{RF}_i(ctr_{|i}))\big)\ ,\ \big(\rho_1,\ \widetilde{\alpha}_{\rho_1}(\overline{\mathsf{RF}}_i(ctr_{|i}))\big) \;\big|\; \widetilde{\alpha}_{\rho_0}(\mathsf{RF}_i(ctr_{|i}))\ \Big) \ \leq\ 2^{-\Omega(\lambda)}.$$

Consequently, $\mathsf{H}_{3.i.2}$ and $\mathsf{H}_{3.i.3}$ are statistically close. By a standard hybrid argument over $ctr \in [Q_e]$, we have that $\big|\Pr_{\mathsf{H}3.i.2}[\mathsf{Bad}] - \Pr_{\mathsf{H}3.i.3}[\mathsf{Bad}]\big| \leq Q_e \cdot 2^{-\Omega(\lambda)}$, thus Claim 9 follows. ∎

Hybrid $\mathsf{H}_{3.i.4}$, $i \in [0, n-1]$: This hybrid is the same as $\mathsf{H}_{3.i.3}$, except that, when answering $\textsc{Dec}\big(C = (x, d, \widehat{\pi}', \widetilde{\pi}')\big)$, for $x \in \mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1}$, the challenger computes the set $\mathcal{S}$ as follows:

- $\mathcal{S} := \big\{ \widetilde{\pi} := \widetilde{\mathsf{Priv}}\big(\mathsf{RF}_{i+1}(ctr_{|i}||b), x, \tau\big) \in \widetilde{\Pi} \;\big|\; ctr \in [Q_e],\ b \in \{0,1\} \big\}$.

Note that the set $\mathcal{S}$ in $\mathsf{H}_{3.i.4}$ contains the set $\mathcal{S}$ in $\mathsf{H}_{3.i.3}$. Thus, this change can only increase the probability of Bad, and we have $\Pr_{\mathsf{H}3.i.3}[\mathsf{Bad}] \leq \Pr_{\mathsf{H}3.i.4}[\mathsf{Bad}]$.

Hybrid $\mathsf{H}_{3.i.5}$, $i \in [0, n-1]$: This hybrid is the same as hybrid $\mathsf{H}_{3.i.4}$, except that, when answering $\textsc{Dec}\big(C = (x, d, \widehat{\pi}', \widetilde{\pi}')\big)$ (to detect the occurrence of Bad), for $x \in \mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1}$, the challenger computes the set $\mathcal{S}$ as follows:

- $\mathcal{S} := \big\{ \widetilde{\pi} := \widetilde{\mathsf{Priv}}\big(\mathsf{RF}_{i+1}(ctr_{|i+1}), x, \tau\big) \in \widetilde{\Pi} \ \big|\ ctr \in [Q_e] \big\}$.

Claim 10. $\big| \Pr_{\mathsf{H}3.i.4}[\mathsf{Bad}] - \Pr_{\mathsf{H}3.i.5}[\mathsf{Bad}] \big| \le Q_d \cdot Q_e \cdot 2^{-\Omega(\lambda)}$.

Proof. For clarity, we denote the set $\mathcal{S}$ in $\mathsf{H}_{3.i.4}$ by $\mathcal{S}_{3.i.4}$ and the set $\mathcal{S}$ in $\mathsf{H}_{3.i.5}$ by $\mathcal{S}_{3.i.5}$. Obviously, $\mathcal{S}_{3.i.5} \subsetneq \mathcal{S}_{3.i.4}$. Let Forge denote the event that $\mathcal{A}$ ever queries $\textsc{Dec}\big(C = (x, d, \widehat{\pi}', \widetilde{\pi}')\big)$, such that $\widetilde{\pi}' \in \mathcal{S}_{3.i.4} \setminus \mathcal{S}_{3.i.5}$. Clearly, hybrid $\mathsf{H}_{3.i.4}$ and hybrid $\mathsf{H}_{3.i.5}$ are the same unless Forge happens, thus

$$\big| \Pr_{\mathsf{H}3.i.4}[\mathsf{Bad}] - \Pr_{\mathsf{H}3.i.5}[\mathsf{Bad}] \big| \le \Pr_{\mathsf{H}3.i.5}[\mathsf{Forge}].$$

We analyze the event Forge in $\mathsf{H}_{3.i.5}$.

- Observe that the information about RF_{i+1} that $\mathcal{A}$ may obtain in $\mathsf{H}_{3.i.5}$ is limited to $\big\{\mathsf{RF}_{i+1}(ctr_{|i+1}) \mid ctr \in [Q_e]\big\}$: in $\textsc{Enc}$, $\mathsf{RF}_{i+1}(ctr_{|i+1})$ is used in the computation of $\widetilde{\pi}^*$; in $\textsc{Dec}$, the challenger will not output M unless $x \in \mathcal{L}_\rho$, and for $x \in \mathcal{L}_\rho$, the computation of $\widetilde{\pi}$ does not involve RF_{i+1}.
- The event Forge occurs in $\mathsf{H}_{3.i.5}$ means that $\mathcal{A}$ ever makes a $\textsc{Dec}$ query $C = (x, d, \widehat{\pi}', \widetilde{\pi}')$ such that $\widetilde{\pi}' \in \mathcal{S}_{3.i.4} \setminus \mathcal{S}_{3.i.5}$ holds.

  For any $\widetilde{\pi} = \widetilde{\mathsf{Priv}}\big(\mathsf{RF}_{i+1}(ctr_{|i}||b), x, \tau\big) \in \mathcal{S}_{3.i.4} \setminus \mathcal{S}_{3.i.5}$, it must hold that $ctr_{|i}||b \notin \big\{ctr_{|i+1} \mid ctr \in [Q_e]\big\}$. Consequently, $\mathsf{RF}_{i+1}(ctr_{|i}||b) \in \widetilde{\mathcal{SK}}$ is not involved in $\textsc{Enc}$ and is completely random to $\mathcal{A}$. Since $\widetilde{\mathsf{QAHPS}}$ is $\langle \bot, \bot \rangle$-universal, $\widetilde{\pi} = \widetilde{\mathsf{Priv}}\big(\mathsf{RF}_{i+1}(ctr_{|i}||b), x, \tau\big) = \widetilde{\Lambda}_{\mathsf{RF}_{i+1}(ctr_{|i}||b)}(x, \tau)$ has enough entropy, i.e.,
  $$\widetilde{\mathbf{H}}_\infty\big(\widetilde{\Lambda}_{\mathsf{RF}_{i+1}(ctr_{|i}||b)}(x, \tau)\big) \ \ge\ \Omega(\lambda).$$
  Thus, for such a $\widetilde{\pi}$, $\widetilde{\pi}' = \widetilde{\pi}$ occurs with probability at most $2^{-\Omega(\lambda)}$. By a union bound over $\widetilde{\pi} \in \mathcal{S}_{3.i.4} \setminus \mathcal{S}_{3.i.5}$, in one $\textsc{Dec}$ query, Forge occurs with probability at most $Q_e \cdot 2^{-\Omega(\lambda)}$.

By a union bound over the Q_d times of $\textsc{Dec}$ queries made by $\mathcal{A}$, we get that $\Pr_{\mathsf{H}3.i.5}[\mathsf{Forge}] \le Q_d \cdot Q_e \cdot 2^{-\Omega(\lambda)}$. Consequently, Claim 10 follows. ▮

Hybrid $\mathsf{H}_{3.i.6}$, $i \in [0, n-1]$: This hybrid is the same as $\mathsf{H}_{3.i.5}$, except that, when answering $\textsc{Dec}\big(C = (x, d, \widehat{\pi}', \widetilde{\pi}')\big)$, the challenger removes the new rule added in hybrid $\mathsf{H}_{3.i.2}$. In other words,

- When $x \notin \mathcal{L}_\rho$, the challenger detects whether Bad occurs (no matter $x \in \mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1}$ or not).

  Obviously, this change can only increase the probability of Bad. Thus, we have

$$\Pr_{\mathsf{H}3.i.5}[\mathsf{Bad}] \le \Pr_{\mathsf{H}3.i.6}[\mathsf{Bad}].$$

Claim 11. $\big| \Pr_{\mathsf{H}3.i.6}[\mathsf{Bad}] - \Pr_{\mathsf{H}3.(i+1)}[\mathsf{Bad}] \big| \le \mathsf{Adv}^{Q_e\text{-}msmp}_{\mathscr{L}_0}(\lambda) + \mathsf{Adv}^{Q_e\text{-}msmp}_{\mathscr{L}_1}(\lambda)$.

The only difference between hybrid $\mathsf{H}_{3.i.6}$ and hybrid $\mathsf{H}_{3.(i+1)}$ lies in the distribution of x^* in $\textsc{Enc}$: for the ctr-th $\textsc{Enc}$ query, where $ctr \in [Q_e]$, $x^* \leftarrow_\$ \mathcal{L}_{\rho_{ctr_{i+1}}}$ in $\mathsf{H}_{3.i.6}$, while $x^* \leftarrow_\$ \mathcal{L}_{\rho_0}$ in $\mathsf{H}_{3.(i+1)}$. The proof of Claim 11 is essentially the same as that for Claim 7, since the change from $\mathsf{H}_{3.i.6}$ to $\mathsf{H}_{3.(i+1)}$ is symmetric to the change from $\mathsf{H}_{3.i}$ to $\mathsf{H}_{3.i.1}$.

Hybrid H_4: It is the same as $\mathsf{H}_{3.\lceil \log Q_e \rceil}$. Thus, $\Pr_{\mathsf{H}3.\lceil \log Q_e \rceil}[\mathsf{Bad}] = \Pr_{\mathsf{H}4}[\mathsf{Bad}]$.

In this hybrid, when answering the ctr-th $\textsc{Enc}$ query, where $ctr \in [Q_e]$, the challenger computes $\widetilde{\pi}^*$ using $\mathsf{RF}_{\lceil \log Q_e \rceil}(ctr)$:

- $\widetilde{\pi}^* := \widetilde{\mathsf{Priv}}\big(\mathsf{RF}_{\lceil \log Q_e \rceil}(ctr), x^*, \tau^*\big) \in \widetilde{\Pi}$.

Moreover, when answering $\textsc{Dec}\big(C = (x, d, \widehat{\pi}', \widetilde{\pi}')\big)$, for $x \notin \mathcal{L}_\rho$, the challenger computes the set $\mathcal{S}$ using $\mathsf{RF}_{\lceil \log Q_e \rceil}(ctr)$ to detect the occurrence of Bad:

- $\mathcal{S} := \big\{ \widetilde{\pi} := \widetilde{\mathsf{Priv}}\big(\mathsf{RF}_{\lceil \log Q_e \rceil}(ctr), x, \tau\big) \in \widetilde{\Pi} \ \big|\ ctr \in [Q_e] \big\}$.

Here $\mathsf{RF}_{\lceil \log Q_e \rceil} : ([Q_e] \subseteq) \{0,1\}^{\lceil \log Q_e \rceil} \longrightarrow \widetilde{\mathcal{SK}}$ is a truly random function implemented by the challenger on the fly.

Claim 12. $\Pr_{\mathsf{H4}}[\mathsf{Bad}] \leq Q_d \cdot Q_e \cdot 2^{-\Omega(\lambda)}$.

Proof. We analyze the event Bad in H_4.

– Observe that the information about $\mathsf{RF}_{\lceil \log Q_e \rceil}$ that $\mathcal{A}$ may obtain in H_4 is limited to $\big\{\mathsf{RF}_{\lceil \log Q_e \rceil}(ctr) \mid ctr \in [Q_e]\big\}$: in the ctr-th Enc query, where $ctr \in [Q_e]$, $\mathsf{RF}_{\lceil \log Q_e \rceil}(ctr)$ is used in the computation of $\widetilde{\pi}^*$; in Dec, the challenger will not output M unless $x \in \mathcal{L}_\rho$, and for $x \in \mathcal{L}_\rho$, the computation of $\widetilde{\pi}$ does not involve $\mathsf{RF}_{\lceil \log Q_e \rceil}$ (recall that it uses $\widetilde{sk}$); Leak only leaks information about $\mathsf{SK} = (sk, \widehat{sk}, \widetilde{sk})$, and for all $ctr \in [Q_e]$, no information about $\mathsf{RF}_{\lceil \log Q_e \rceil}(ctr)$ is leaked to $\mathcal{A}$.

– The event Bad occurs in H_4 implies that $\mathcal{A}$ ever makes a Dec query $C = (x, d, \widehat{\pi}', \widetilde{\pi}')$ such that $\tau \notin \mathcal{Q}_{\mathcal{TAG}} \ \wedge \ x \notin \mathcal{L}_\rho$ but $\widetilde{\pi}' \in \mathcal{S}$ hold.

  For any $\widetilde{\pi} = \widetilde{\mathsf{Priv}}\big(\mathsf{RF}_{\lceil \log Q_e \rceil}(ctr), x, \tau\big) \in \mathcal{S}$, we observe that $\mathsf{RF}_{\lceil \log Q_e \rceil}(ctr) \in \widetilde{\mathcal{SK}}$ is only used once in the ctr-th Enc query for computing $\widetilde{\pi}^* := \widetilde{\mathsf{Priv}}\big(\mathsf{RF}_{\lceil \log Q_e \rceil}(ctr), x^*, \tau^*\big) = \widetilde{\Lambda}_{\mathsf{RF}_{\lceil \log Q_e \rceil}(ctr)}(x^*, \tau^*) \in \widetilde{\Pi}$. Recall that, tag-based $\widetilde{\mathsf{QAHPS}}$ is $\langle \bot, \bot \rangle$-universal and $\tau \neq \tau^*$, so $\widetilde{\pi} = \widetilde{\mathsf{Priv}}\big(\mathsf{RF}_{\lceil \log Q_e \rceil}(ctr), x, \tau\big) = \widetilde{\Lambda}_{\mathsf{RF}_{\lceil \log Q_e \rceil}(ctr)}(x, \tau)$ has enough entropy even conditioned on $\widetilde{\pi}^*$, i.e.,

$$\widetilde{\mathbf{H}}_\infty\big(\widetilde{\Lambda}_{\mathsf{RF}_{\lceil \log Q_e \rceil}(ctr)}(x, \tau) \;\big|\; \widetilde{\Lambda}_{\mathsf{RF}_{\lceil \log Q_e \rceil}(ctr)}(x^*, \tau^*)\big) \ \geq \ \Omega(\lambda).$$

  In this case, $\widetilde{\pi}' = \widetilde{\pi}$ occurs with probability at most $2^{-\Omega(\lambda)}$. By a union bound over $\widetilde{\pi} \in \mathcal{S}$, in one Dec query, Bad occurs with probability at most $Q_e \cdot 2^{-\Omega(\lambda)}$.

By a union bound over the Q_d times of Dec queries made by $\mathcal{A}$, we get that $\Pr_{\mathsf{H4}}[\mathsf{Bad}] \leq Q_d \cdot Q_e \cdot 2^{-\Omega(\lambda)}$, thus Claim 12 follows. ▌

All in all, by combining (10), (11) and the above claims, Lemma 8 follows. □

5 Instantiations over Asymmetric Pairing Groups

Now we instantiate our generic PKE construction in Sect. 4 based on the matrix DDH assumptions over asymmetric pairing groups. Specifically, we present the instantiations of the language distributions $\mathscr{L}, \mathscr{L}_0, \mathscr{L}_1$, the LR-weak-ardent QAHPS, the LR-ardent $\widehat{\mathsf{QAHPS}}$, the LR-weak-ardent tag-based $\widetilde{\mathsf{QAHPS}}$ and the resulting scheme $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{asym}}$, in Subsects. 5.2, 5.3, 5.4, 5.5, and 5.6, respectively.

5.1 The Language Distribution for Linear Subspaces

Let $\mathcal{PG} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, e, P_1, P_2, P_T)$ be an asymmetric pairing group. For any matrix distribution $\mathcal{D}_{\ell,k}$, which outputs matrices in $\mathbb{Z}_p^{\ell \times k}$, it naturally gives rise to a language distribution $\mathscr{L}_{\mathcal{D}_{\ell,k}}$ for linear subspaces over groups $\mathbb{G}_1$ and $\mathbb{G}_2$:

– $\mathscr{L}_{\mathcal{D}_{\ell,k}}$ invokes $\mathbf{A}_1, \mathbf{A}_2 \leftarrow_{\$} \mathcal{D}_{\ell,k}$, and outputs a language parameter $\rho = ([\mathbf{A}_1]_1, [\mathbf{A}_2]_2) \in \mathbb{G}_1^{\ell \times k} \times \mathbb{G}_2^{\ell \times k}$ together with a trapdoor $td = (\mathbf{A}_1, \mathbf{A}_2)$.

The matrix ρ defines a linear subspace language $\mathcal{L}_\rho$ on $\mathbb{G}_1^\ell \times \mathbb{G}_2^\ell$:

$$\begin{aligned}\mathcal{L}_\rho &= \big\{ \ ([\mathbf{c}_1]_1, [\mathbf{c}_2]_2) \ \big| \ \exists \ \mathbf{w}_1, \mathbf{w}_2 \in \mathbb{Z}_p^k \setminus \{\mathbf{0}\}, \ \text{s.t.} \ [\mathbf{c}_1]_1 = [\mathbf{A}_1 \mathbf{w}_1]_1 \ \wedge \ [\mathbf{c}_2]_2 = [\mathbf{A}_2 \mathbf{w}_2]_2 \ \big\} \\ &= \mathsf{span}([\mathbf{A}_1]_1) \times \mathsf{span}([\mathbf{A}_2]_2) \ \subseteq \mathcal{X} = \big(\mathbb{G}_1^\ell \setminus \{[\mathbf{0}]_1\}\big) \times \big(\mathbb{G}_2^\ell \setminus \{[\mathbf{0}]_2\}\big).\end{aligned}$$ [8]

[8] For technical reasons, the zero vector $[\mathbf{0}]_1$ (resp. $[\mathbf{0}]_2$) must be excluded from $\mathsf{span}([\mathbf{A}_1]_1)$ and $\mathbb{G}_1^\ell$ (resp. $\mathsf{span}([\mathbf{A}_2]_2)$ and $\mathbb{G}_2^\ell$). For the sake of simplicity, we forgo making this explicit in the sequel.

The trapdoor td can be used to decide whether or not an instance $([\mathbf{c}_1]_1, [\mathbf{c}_2]_2)$ is in $\mathcal{L}_\rho$ efficiently: with $td = (\mathbf{A}_1, \mathbf{A}_2)$, one can first compute a basis of the kernel space of $\mathbf{A}_1^\top$ (resp. $\mathbf{A}_2^\top$), namely $\mathbf{A}_1^\perp \in \mathbb{Z}_p^{\ell\times(\ell-k)}$ satisfying $\mathbf{A}_1^\top \cdot \mathbf{A}_1^\perp = \mathbf{0}$ (resp. $\mathbf{A}_2^\perp \in \mathbb{Z}_p^{\ell\times(\ell-k)}$ satisfying $\mathbf{A}_2^\top \cdot \mathbf{A}_2^\perp = \mathbf{0}$), then check whether $[\mathbf{c}_1^\top]_1 \cdot \mathbf{A}_1^\perp = [\mathbf{0}]_1 \ \wedge\ [\mathbf{c}_2^\top]_2 \cdot \mathbf{A}_2^\perp = [\mathbf{0}]_2$ holds.

Clearly, the SMP related to $\mathscr{L}_{\mathcal{D}_{\ell,k}}$ corresponds to a hybrid of the $\mathcal{D}_{\ell,k}$-MDDH assumptions over $\mathbb{G}_1$ and $\mathbb{G}_2$, and the multi-fold SMP related to $\mathscr{L}_{\mathcal{D}_{\ell,k}}$ corresponds to a hybrid of the Q-fold $\mathcal{D}_{\ell,k}$-MDDH assumptions over $\mathbb{G}_1$ and $\mathbb{G}_2$ for any $Q = \mathsf{poly}(\lambda)$. The same also holds for the uniform distribution $\mathcal{U}_{\ell,k}$. Formally, we have the following lemma, which is a corollary of the random self-reducibility of $\mathcal{D}_{\ell,k}$-MDDH and $\mathcal{U}_{\ell,k}$-MDDH (i.e., Lemma 6).

Lemma 9 ($\mathcal{D}_{\ell,k}/\mathcal{U}_{\ell,k}$-MDDH $\Rightarrow$ Multi-fold SMP related to $\mathscr{L}_{\mathcal{D}_{\ell,k}}/\mathscr{L}_{\mathcal{U}_{\ell,k}}$). *Let $Q > \ell - k$. For any adversary $\mathcal{A}$, there exist adversaries $\mathcal{B}_1$ and $\mathcal{B}_2$ such that $\mathbf{T}(\mathcal{B}_1) \approx \mathbf{T}(\mathcal{B}_2) \approx \mathbf{T}(\mathcal{A}) + Q\cdot\mathsf{poly}(\lambda)$ with $\mathsf{poly}(\lambda)$ independent of $\mathbf{T}(\mathcal{A})$, and*

$$\mathsf{Adv}^{Q\text{-}msmp}_{\mathscr{L}_{\mathcal{D}_{\ell,k}},\mathcal{A}}(\lambda) \ \le\ (\ell-k)\cdot\mathsf{Adv}^{mddh}_{\mathcal{D}_{\ell,k},\mathbb{G}_1,\mathcal{B}_1}(\lambda) + (\ell-k)\cdot\mathsf{Adv}^{mddh}_{\mathcal{D}_{\ell,k},\mathbb{G}_2,\mathcal{B}_2}(\lambda) + 2/(p-1).$$

For any adversary $\mathcal{A}$, there exist adversaries $\mathcal{B}_1$ and $\mathcal{B}_2$ such that $\mathbf{T}(\mathcal{B}_1) \approx \mathbf{T}(\mathcal{B}_2) \approx \mathbf{T}(\mathcal{A}) + Q\cdot\mathsf{poly}(\lambda)$ with $\mathsf{poly}(\lambda)$ independent of $\mathbf{T}(\mathcal{A})$, and

$$\mathsf{Adv}^{Q\text{-}msmp}_{\mathscr{L}_{\mathcal{U}_{\ell,k}},\mathcal{A}}(\lambda) \ \le\ \mathsf{Adv}^{mddh}_{\mathcal{U}_{\ell,k},\mathbb{G}_1,\mathcal{B}_1}(\lambda) + \mathsf{Adv}^{mddh}_{\mathcal{U}_{\ell,k},\mathbb{G}_2,\mathcal{B}_2}(\lambda) + 2/(p-1).$$

5.2 The Instantiation of Language Distributions

To instantiate the generic PKE construction in Sect. 4, the first thing we need to do is to determine three language distributions $\mathscr{L}$, $\mathscr{L}_0$ and $\mathscr{L}_1$ carefully.

Let $\ell \ge 2k+1$. Let $\mathcal{D}_{\ell,k}$ be an (arbitrary) matrix distribution, and $\mathcal{U}_{\ell,k}$, $\mathcal{U}'_{\ell,k}$ independent copies of the uniform distribution, all of which output matrices in $\mathbb{Z}_p^{\ell\times k}$. Based on the previous subsection, we designate the language distributions $\mathscr{L}$, $\mathscr{L}_0$ and $\mathscr{L}_1$ as follows.

- $\mathscr{L} := \mathscr{L}_{\mathcal{D}_{\ell,k}}$, which invokes $\mathbf{A}_1, \mathbf{A}_2 \leftarrow_{\$} \mathcal{D}_{\ell,k}$ and outputs $(\rho = ([\mathbf{A}_1]_1, [\mathbf{A}_2]_2), td = (\mathbf{A}_1, \mathbf{A}_2))$;
- $\mathscr{L}_0 := \mathscr{L}_{\mathcal{U}_{\ell,k}}$, which invokes $\mathbf{A}_{0,1}, \mathbf{A}_{0,2} \leftarrow_{\$} \mathcal{U}_{\ell,k}$ and outputs $(\rho_0 = ([\mathbf{A}_{0,1}]_1, [\mathbf{A}_{0,2}]_2), td_0 = (\mathbf{A}_{0,1}, \mathbf{A}_{0,2}))$;
- $\mathscr{L}_1 := \mathscr{L}_{\mathcal{U}'_{\ell,k}}$, which invokes $\mathbf{A}_{1,1}, \mathbf{A}_{1,2} \leftarrow_{\$} \mathcal{U}'_{\ell,k}$ and outputs $(\rho_1 = ([\mathbf{A}_{1,1}]_1, [\mathbf{A}_{1,2}]_2), td_1 = (\mathbf{A}_{1,1}, \mathbf{A}_{1,2}))$.

5.3 The Instantiation of LR-Weak-Ardent QAHPS

We present the construction of $\mathsf{QAHPS} = (\mathsf{Setup}, \alpha_{(\cdot)}, \mathsf{Pub}, \mathsf{Priv})$ for the language distribution $\mathscr{L}$ $(= \mathscr{L}_{\mathcal{D}_{\ell,k}})$ in Fig. 3. It is straightforward to check the perfect correctness of QAHPS.

Theorem 2 ($\mathscr{L}_0$-Multi-Extracting of QAHPS). *If the $\mathcal{U}_{k+1,k}$-MDDH assumption holds over $\mathbb{G}_2$, then the proposed QAHPS in Fig. 3 is $\mathscr{L}_0$-multi-extracting, where the language distribution $\mathscr{L}_0$ $(= \mathscr{L}_{\mathcal{U}_{\ell,k}})$ is specified in Subsect. 5.2.*

Concretely, for any adversary $\mathcal{A}$, any polynomial $Q = \mathsf{poly}(\lambda)$, there exists an adversary $\mathcal{B}$, such that $\mathbf{T}(\mathcal{B}) \approx \mathbf{T}(\mathcal{A}) + Q\cdot\mathsf{poly}(\lambda)$ with $\mathsf{poly}(\lambda)$ independent of $\mathbf{T}(\mathcal{A})$, and

$$\mathsf{Adv}^{Q\text{-}\mathscr{L}_0\text{-}mext}_{\mathsf{QAHPS},\mathcal{A}}(\lambda) \le \mathsf{Adv}^{mddh}_{\mathcal{U}_{k+1,k},\mathbb{G}_2,\mathcal{B}}(\lambda) + 1/(p-1).$$

Proof of Theorem 2. Firstly, we construct an adversary $\mathcal{B}'$ against the Q-fold $\mathcal{U}_{k+1,k}$-MDDH over $\mathbb{G}_2$, so that $\mathsf{Adv}^{Q\text{-}\mathscr{L}_0\text{-}mext}_{\mathsf{QAHPS},\mathcal{A}}(\lambda) \le \mathsf{Adv}^{Q\text{-}mddh}_{\mathcal{U}_{k+1,k},\mathbb{G}_2,\mathcal{B}'}(\lambda)$. Then by the random self-reducibility of $\mathcal{U}_{k+1,k}$-MDDH (i.e., Lemma 6), Theorem 2 follows.

Given a challenge $([\mathbf{B}]_2, [\mathbf{U}]_2)$, $\mathcal{B}'$ wants to distinguish $[\mathbf{U}]_2 = [\mathbf{B}\mathbf{W}]_2$ from $[\mathbf{U}]_2 \leftarrow_{\$} \mathbb{G}_2^{(k+1)\times Q}$, where $\mathbf{B} \leftarrow_{\$} \mathcal{U}_{k+1,k}$, $\mathbf{W} \leftarrow_{\$} \mathbb{Z}_p^{k\times Q}$. Let $[\mathbf{u}_j]_2 \in \mathbb{G}_2^{k+1}$ denote the j-th column of $[\mathbf{U}]_2$, $j \in [Q]$. $\mathcal{B}'$ is constructed as follows.

$pp \leftarrow_\$ \mathsf{Setup}(1^\lambda)$: $\mathcal{PG} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, e, P_1, P_2, P_T) \leftarrow_\$ \mathsf{PGGen}(1^\lambda)$. $\Rightarrow pp := \mathcal{PG}$, which implicitly defines $(\mathcal{SK} := \mathbb{Z}_p^\ell,\ \Pi := \mathbb{G}_2,\ \Lambda_{(\cdot)})$, where $\Lambda_{sk}([\mathbf{c}_1]_1, [\mathbf{c}_2]_2) := \mathbf{k}^\top \cdot [\mathbf{c}_2]_2 \in \mathbb{G}_2$ for any $sk = \mathbf{k} \in \mathbb{Z}_p^\ell$ and $([\mathbf{c}_1]_1, [\mathbf{c}_2]_2) \in \mathcal{X} = \mathbb{G}_1^\ell \times \mathbb{G}_2^\ell$.	$pk_\rho \leftarrow \alpha_\rho(sk)$, where $\rho = ([\mathbf{A}_1]_1, [\mathbf{A}_2]_2) \in \mathbb{G}_1^{\ell\times k} \times \mathbb{G}_2^{\ell\times k}$: Parse $sk = \mathbf{k} \in \mathbb{Z}_p^\ell$. $[\mathbf{p}^\top]_2 := \mathbf{k}^\top \cdot [\mathbf{A}_2]_2 \in \mathbb{G}_2^{1\times k}$. $\Rightarrow pk_\rho := [\mathbf{p}^\top]_2$.
$[\pi]_2 \leftarrow \mathsf{Pub}(pk_\rho, ([\mathbf{c}_1]_1, [\mathbf{c}_2]_2), (\mathbf{w}_1, \mathbf{w}_2) \in \mathbb{Z}_p^k \times \mathbb{Z}_p^k)$, where $([\mathbf{c}_1]_1, [\mathbf{c}_2]_2) \in \mathcal{L}_\rho$ for $\rho = ([\mathbf{A}_1]_1, [\mathbf{A}_2]_2)$: Parse $pk_\rho = [\mathbf{p}^\top]_2 \in \mathbb{G}_2^{1\times k}$. $\Rightarrow [\pi]_2 := [\mathbf{p}^\top]_2 \cdot \mathbf{w}_2 \in \mathbb{G}_2$.	$[\pi]_2 \leftarrow \mathsf{Priv}(sk, ([\mathbf{c}_1]_1, [\mathbf{c}_2]_2) \in \mathcal{X})$: Parse $sk = \mathbf{k} \in \mathbb{Z}_p^\ell$. $\Rightarrow [\pi]_2 := \mathbf{k}^\top \cdot [\mathbf{c}_2]_2 \in \mathbb{G}_2$.

Fig. 3. Construction of LR-weak-ardent QAHPS over asymmetric pairing groups.

- $\mathcal{B}'$ chooses $\mathbf{V} \leftarrow_\$ \mathbb{Z}_p^{\ell\times k}$ uniformly, computes $[\mathbf{A}_{0,2}]_2 := \mathbf{V}[\overline{\mathbf{B}}]_2 \in \mathbb{G}_2^{\ell\times k}$, picks $\mathbf{A}_{0,1} \leftarrow_\$ \mathcal{U}_{\ell,k}$, and sets $\rho_0 := ([\mathbf{A}_{0,1}]_1, [\mathbf{A}_{0,2}]_2)$ as the language parameter.
- $\mathcal{B}'$ implicitly sets $sk = \mathbf{k} \leftarrow_\$ \mathbb{Z}_p^\ell$ with $\mathbf{k}^\top \cdot [\mathbf{A}_{0,2}]_2 = [\underline{\mathbf{B}}]_2$.
- For each $[\mathbf{u}_j]_2$, $\mathcal{B}'$ computes $[\mathbf{c}_{2,j}]_2 := \mathbf{V}[\overline{\mathbf{u}_j}]_2 \in \mathbb{G}_2^\ell$ and $[\pi_j]_2 := [\underline{\mathbf{u}_j}]_2 \in \mathbb{G}_2$, samples $\mathbf{r}_j \leftarrow_\$ \mathbb{Z}_p^k$, and computes $[\mathbf{c}_{1,j}]_1 = [\mathbf{A}_{0,1}\mathbf{r}_j]_1$.
- Finally, $\mathcal{B}'$ submits $\big(\ \rho_0,\ \big\{([\mathbf{c}_{1,j}]_1, [\mathbf{c}_{2,j}]_2),\ [\pi_j]_2\big\}_{j\in[Q]}\ \big)$ to $\mathcal{A}$, and outputs whatever $\mathcal{A}$ outputs.

Clearly, $[\mathbf{A}_{0,2}]_2$ is uniformly distributed over $\mathbb{G}_2^{\ell\times k}$, due to the randomness of $\mathbf{V}$. Thus the simulation of $\rho_0 = ([\mathbf{A}_{0,1}]_1, [\mathbf{A}_{0,2}]_2)$ is perfect. Besides, the simulation of $sk = \mathbf{k}$ is perfect due to the randomness of $\underline{\mathbf{B}} \in \mathbb{Z}_p^{1\times k}$.

- If $[\mathbf{U}]_2 = [\mathbf{B}\mathbf{W}]_2$, then each $[\mathbf{u}_j]_2 = [\mathbf{B}\mathbf{w}_j]_2$ with $\mathbf{w}_j \leftarrow_\$ \mathbb{Z}_p^k$. Consequently,
  - $[\mathbf{c}_{2,j}]_2 := \mathbf{V}[\overline{\mathbf{u}_j}]_2 = [\mathbf{V}\overline{\mathbf{B}}\mathbf{w}_j]_2 = [\mathbf{A}_{0,2}\mathbf{w}_j]_2$. Together with $[\mathbf{c}_{1,j}]_1 = [\mathbf{A}_{0,1}\mathbf{r}_j]_1$, we have $([\mathbf{c}_{1,j}]_1, [\mathbf{c}_{2,j}]_2)$ is uniformly distributed over $\mathsf{span}([\mathbf{A}_{0,1}]_1) \times \mathsf{span}([\mathbf{A}_{0,2}]_2) = \mathcal{L}_{\rho_0}$.
  - $[\pi_j]_2 := [\underline{\mathbf{u}_j}]_2 = [\underline{\mathbf{B}}\mathbf{w}_j]_2 = \mathbf{k}^\top \cdot [\mathbf{A}_{0,2}\mathbf{w}_j]_2 = \mathbf{k}^\top \cdot [\mathbf{c}_{2,j}]_2 = \Lambda_{sk}([\mathbf{c}_{1,j}]_1, [\mathbf{c}_{2,j}]_2)$.
- If $[\mathbf{U}]_2 \leftarrow_\$ \mathbb{G}^{(k+1)\times Q}$, then each $[\mathbf{u}_j]_2 \leftarrow_\$ \mathbb{G}_2^{k+1}$.
  - $[\mathbf{c}_{2,j}]_2 := \mathbf{V}[\overline{\mathbf{u}_j}]_2 = [\mathbf{V}\overline{\mathbf{B}}\,\overline{\mathbf{B}}^{-1}\overline{\mathbf{u}_j}]_2 = [\mathbf{A}_{0,2}\overline{\mathbf{B}}^{-1}\overline{\mathbf{u}_j}]_2$ which is uniformly distributed over $\mathsf{span}([\mathbf{A}_{0,2}]_2)$. Together with $[\mathbf{c}_{1,j}]_1 = [\mathbf{A}_{0,1}\mathbf{r}_j]_1$, we have $([\mathbf{c}_{1,j}]_1, [\mathbf{c}_{2,j}]_2)$ is uniformly distributed over $\mathcal{L}_{\rho_0}$.
  - $[\pi_j]_2 := [\underline{\mathbf{u}_j}]_2 \in \mathbb{G}_2$, which is uniformly distributed over $\Pi = \mathbb{G}_2$ (and in particular, is independent of $([\mathbf{c}_{1,j}]_1, [\mathbf{c}_{2,j}]_2)$).

Consequently, we get $\mathsf{Adv}^{Q\text{-}\mathscr{L}_0\text{-}mext}_{\mathsf{QAHPS},\mathcal{A}}(\lambda) \le \mathsf{Adv}^{Q\text{-}mddh}_{\mathcal{U}_{k+1,k},\mathbb{G}_2,\mathcal{B}'}(\lambda)$, as desired. This completes the proof of Theorem 2. □

The LR-weak-ardency of QAHPS follows from the theorem below.

Theorem 3 (LR-weak-ardency of QAHPS). *Let $\ell \ge 2k+1$ and $\kappa \le \log p - \Omega(\lambda)$. The proposed QAHPS for $\mathscr{L}$ in Fig. 3 satisfies the properties listed in Table 2, i.e., (1) it is perfectly $\langle\perp,\perp\rangle$-universal and (2) it supports κ-LR-$\langle\mathscr{L},\mathscr{L}_0\rangle$-key-switching, where the language distributions $\mathscr{L} = \mathscr{L}_{\mathcal{D}_{\ell,k}}$ and $\mathscr{L}_0 = \mathscr{L}_{\mathcal{U}_{\ell,k}}$ are specified in Subsect. 5.2.*

Proof of Theorem 3. Let $(\rho = ([\mathbf{A}_1]_1, [\mathbf{A}_2]_2) \in \mathbb{G}_1^{\ell\times k} \times \mathbb{G}_2^{\ell\times k}, td) \leftarrow_\$ \mathscr{L}$ and $(\rho_0 = ([\mathbf{A}_{0,1}]_1, [\mathbf{A}_{0,2}]_2) \in \mathbb{G}_1^{\ell\times k} \times \mathbb{G}_2^{\ell\times k}, td_0) \leftarrow_\$ \mathscr{L}_0$. With overwhelming probability $1 - 2^{-\Omega(\lambda)}$, both $(\mathbf{A}_1, \mathbf{A}_{0,1}) \in \mathbb{Z}_p^{\ell\times 2k}$ and $(\mathbf{A}_2, \mathbf{A}_{0,2}) \in \mathbb{Z}_p^{\ell\times 2k}$ are of full column rank. In the following analysis, we take it for granted.

[Perfectly $\langle\perp,\perp\rangle$-Universal.] For $sk = \mathbf{k} \leftarrow_\$ \mathbb{Z}_p^\ell$ and any $([\mathbf{c}_1]_1, [\mathbf{c}_2]_2) \in \mathcal{X} \setminus (\mathcal{L}_{\rho_\perp} \cup \mathcal{L}_{\rho_\perp}) = \mathcal{X}$, we have $[\mathbf{c}_2]_2 \ne [\mathbf{0}]_2$ (recall that $\mathbb{G}_1^\ell \times \{[\mathbf{0}]_2\}$ is excluded from $\mathcal{X}$), thus $\Lambda_{sk}([\mathbf{c}_1]_1, [\mathbf{c}_2]_2) = \mathbf{k}^\top \cdot [\mathbf{c}_2]_2$ is uniformly distributed over $\mathbb{G}_2$. This implies that QAHPS is perfectly $\langle\perp,\perp\rangle$-universal.

[**κ-LR-$\langle \mathscr{L}, \mathscr{L}_0 \rangle$-Key-Switching.**] Let $L : \mathcal{SK} \longrightarrow \{0,1\}^\kappa$ be an arbitrary leakage function. For $sk = \mathbf{k} \leftarrow_\$ \mathbb{Z}_p^\ell$, $sk' = \mathbf{k}' \leftarrow_\$ \mathbb{Z}_p^\ell$, we aim to prove

$$\Delta\Big(\big(\rho_0, \underbrace{\boxed{\mathbf{k}^\top [\mathbf{A}_{0,2}]_2}}_{\alpha_{\rho_0}(sk)} \big), \big(\rho_0, \underbrace{\boxed{\mathbf{k}'^\top [\mathbf{A}_{0,2}]_2}}_{\alpha_{\rho_0}(sk')} \big) \;\Big|\; \underbrace{\mathbf{k}^\top [\mathbf{A}_2]_2}_{\alpha_\rho(sk)}, \; L(\mathbf{k}) \Big) \leq 2^{-\Omega(\lambda)}. \tag{12}$$

Taking $[\mathbf{A}_{0,2}]_2$ as a universal hash function and $\mathbf{k}$ as an independent input, we have that

$$\Delta\Big(\big([\mathbf{A}_{0,2}]_2, \boxed{\mathbf{k}^\top [\mathbf{A}_{0,2}]_2}\big), \big([\mathbf{A}_{0,2}]_2, \boxed{[\mathbf{u}^\top]_2}\big) \;\Big|\; \mathbf{k}^\top [\mathbf{A}_2]_2, \; L(\mathbf{k}) \Big) \leq 2^{-\Omega(\lambda)}. \tag{13}$$

where $\mathbf{u} \leftarrow_\$ \mathbb{Z}_p^k$, by the generalized leftover hash lemma (i.e., Lemma 3). Meanwhile, $\mathbf{k}'$ is uniform and independent of $\mathbf{A}_{0,2}, \mathbf{A}_2$ and $\mathbf{k}$. So,

$$\big([\mathbf{A}_{0,2}]_2, \boxed{[\mathbf{u}^\top]_2}, \mathbf{k}^\top [\mathbf{A}_2]_2, \; L(\mathbf{k}) \big) \equiv \big([\mathbf{A}_{0,2}]_2, \boxed{\mathbf{k}'^\top [\mathbf{A}_{0,2}]_2}, \mathbf{k}^\top [\mathbf{A}_2]_2, \; L(\mathbf{k}) \big). \tag{14}$$

(13) and (14) implies

$$\Delta\Big(\big([\mathbf{A}_{0,2}]_2, \mathbf{k}^\top [\mathbf{A}_{0,2}]_2\big), \big([\mathbf{A}_{0,2}]_2, \mathbf{k}'^\top [\mathbf{A}_{0,2}]_2\big) \;\Big|\; \mathbf{k}^\top [\mathbf{A}_2]_2, \; L(\mathbf{k}) \Big) \leq 2^{-\Omega(\lambda)}.$$

(12) follows from the fact that $\mathbf{A}_{0,1}$ is independent of $\mathbf{A}_{0,2}, \mathbf{A}_2, \mathbf{k}$ and $\mathbf{k}'$.

This completes the proof of κ-LR-$\langle \mathscr{L}, \mathscr{L}_0 \rangle$-key-switching. □

5.4 The Instantiation of LR-Ardent QAHPS

We present the construction of $\widehat{\mathsf{QAHPS}} = (\widehat{\mathsf{Setup}}, \widehat{\alpha}_{(\cdot)}, \widehat{\mathsf{Pub}}, \widehat{\mathsf{Priv}})$ for $\mathscr{L}$ $(= \mathscr{L}_{\mathcal{D}_{\ell,k}})$ in Fig. 4. It is straightforward to check the perfect correctness of $\widehat{\mathsf{QAHPS}}$. The construction is inspired by the "OR-proof" proposed in [ABP15] and the QA-NIZK for linear subspaces proposed in [KW15].

$\widehat{pp} \leftarrow_\$ \widehat{\mathsf{Setup}}(1^\lambda)$: $\mathcal{PG} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, e, P_1, P_2, P_T) \leftarrow_\$ \mathsf{PGGen}(1^\lambda)$. $\Rightarrow \widehat{pp} := \mathcal{PG}$, which implicitly defines $(\widehat{\mathcal{SK}} := \mathbb{Z}_p^{\ell\times\ell}, \; \widehat{\Pi} := \mathbb{G}_T, \; \widehat{\Lambda}_{(\cdot)})$, where $\widehat{\Lambda}_{\widehat{sk}}([\mathbf{c}_1]_1, [\mathbf{c}_2]_2) := [\mathbf{c}_2]_2^\top \cdot \widehat{\mathbf{K}} \cdot [\mathbf{c}_1]_1 \in \mathbb{G}_T$ for any $\widehat{sk} = \widehat{\mathbf{K}} \in \mathbb{Z}_p^{\ell\times\ell}$ and $([\mathbf{c}_1]_1, [\mathbf{c}_2]_2) \in \mathcal{X} = \mathbb{G}_1^\ell \times \mathbb{G}_2^\ell$.	$\widehat{pk}_\rho \leftarrow \widehat{\alpha}_\rho(\widehat{sk})$, where $\rho = ([\mathbf{A}_1]_1, [\mathbf{A}_2]_2) \in \mathbb{G}_1^{\ell\times k} \times \mathbb{G}_2^{\ell\times k}$: Parse $\widehat{sk} = \widehat{\mathbf{K}} \in \mathbb{Z}_p^{\ell\times\ell}$. $[\widehat{\mathbf{P}}]_T := [\mathbf{A}_2]_2^\top \cdot \widehat{\mathbf{K}} \cdot [\mathbf{A}_1]_1 \in \mathbb{G}_T^{k\times k}$. $\Rightarrow \widehat{pk}_\rho := [\widehat{\mathbf{P}}]_T$.
$[\widehat{\pi}]_T \leftarrow \widehat{\mathsf{Pub}}(\widehat{pk}_\rho, ([\mathbf{c}_1]_1, [\mathbf{c}_2]_2), (\mathbf{w}_1, \mathbf{w}_2) \in \mathbb{Z}_p^k \times \mathbb{Z}_p^k)$, where $([\mathbf{c}_1]_1, [\mathbf{c}_2]_2) \in \mathcal{L}_\rho$ for $\rho = ([\mathbf{A}_1]_1, [\mathbf{A}_2]_2)$: Parse $\widehat{pk}_\rho = [\widehat{\mathbf{P}}]_T \in \mathbb{G}_T^{k\times k}$. $\Rightarrow [\widehat{\pi}]_T := \mathbf{w}_2^\top \cdot [\widehat{\mathbf{P}}]_T \cdot \mathbf{w}_1 \in \mathbb{G}_T$.	$[\widehat{\pi}]_T \leftarrow \widehat{\mathsf{Priv}}(\widehat{sk}, ([\mathbf{c}_1]_1, [\mathbf{c}_2]_2) \in \mathcal{X})$: Parse $\widehat{sk} = \widehat{\mathbf{K}} \in \mathbb{Z}_p^{\ell\times\ell}$. $\Rightarrow [\widehat{\pi}]_T := [\mathbf{c}_2]_2^\top \cdot \widehat{\mathbf{K}} \cdot [\mathbf{c}_1]_1 \in \mathbb{G}_T$.

Fig. 4. Construction of LR-ardent $\widehat{\mathsf{QAHPS}}$ over asymmetric pairing groups.

The hash function $\widehat{\Lambda}_{\widehat{sk}}([\mathbf{c}_1]_1, [\mathbf{c}_2]_2)$ multiplies $\widehat{\mathbf{K}}$ with $[\mathbf{c}_1]_1$ and $[\mathbf{c}_2]_2$. The LR-ardency of $\widehat{\mathsf{QAHPS}}$ is proved in Theorem 4.

Theorem 4 (LR-ardency of $\widehat{\mathsf{QAHPS}}$). *Let $\ell \geq 2k+1$ and $\kappa \leq \log p - \Omega(\lambda)$. The proposed $\widehat{\mathsf{QAHPS}}$ scheme for $\mathscr{L}$ in Fig. 4 satisfies the properties listed in Table 2, more precisely, (1) it is κ-LR-$\langle \mathscr{L}, \mathscr{L}_0 \rangle$- and perfectly $\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-universal and (2) it supports κ-LR-$\langle \mathscr{L}, \mathscr{L}_0 \rangle$-key-switching, where the language distributions $\mathscr{L} = \mathscr{L}_{\mathcal{D}_{\ell,k}}$, $\mathscr{L}_0 = \mathscr{L}_{\mathcal{U}_{\ell,k}}$ and $\mathscr{L}_1 = \mathscr{L}_{\mathcal{U}'_{\ell,k}}$ are specified in Subsect. 5.2.*

Proof of Theorem 4.

[Perfectly $\langle\mathscr{L},\mathscr{L}_0\rangle$-Universal.] Let $(\rho = ([\mathbf{A}_1]_1,[\mathbf{A}_2]_2) \in \mathbb{G}_1^{\ell\times k}\times\mathbb{G}_2^{\ell\times k}, td) \leftarrow_{\$} \mathscr{L}$ and $(\rho_0 = ([\mathbf{A}_{0,1}]_1,[\mathbf{A}_{0,2}]_2) \in \mathbb{G}_1^{\ell\times k}\times\mathbb{G}_2^{\ell\times k}, td_0) \leftarrow_{\$} \mathscr{L}_0$. With overwhelming probability $1-2^{-\Omega(\lambda)}$, both $(\mathbf{A}_1,\mathbf{A}_{0,1}) \in \mathbb{Z}_p^{\ell\times 2k}$ and $(\mathbf{A}_2,\mathbf{A}_{0,2}) \in \mathbb{Z}_p^{\ell\times 2k}$ are of full column rank. For $\widehat{sk} = \widehat{\mathbf{K}} \leftarrow_{\$} \mathbb{Z}_p^{\ell\times\ell}$ and any $([\mathbf{c}_1]_1,[\mathbf{c}_2]_2) \in \mathcal{X}\setminus(\mathcal{L}_\rho\cup\mathcal{L}_{\rho_0})$, we consider the distribution of $\widehat{\Lambda}_{\widehat{sk}}([\mathbf{c}_1]_1,[\mathbf{c}_2]_2)$ conditioned on $\widehat{pk}_\rho = \widehat{\alpha}_\rho(\widehat{sk})$ and $\widehat{pk}_{\rho_0} = \widehat{\alpha}_{\rho_0}(\widehat{sk})$.

Let $\mathbf{a}_1^\perp \in \mathbb{Z}_p^\ell$ (resp. $\mathbf{a}_2^\perp \in \mathbb{Z}_p^\ell$, $\mathbf{a}_{0,1}^\perp \in \mathbb{Z}_p^\ell$, $\mathbf{a}_{0,2}^\perp \in \mathbb{Z}_p^\ell$) be an arbitrary non-zero vector in the kernel space of $\mathbf{A}_1^\top$ (resp. $\mathbf{A}_2^\top$, $\mathbf{A}_{0,1}^\top$, $\mathbf{A}_{0,2}^\top$) such that $\mathbf{A}_1^\top\cdot\mathbf{a}_1^\perp = \mathbf{0}$ (resp. $\mathbf{A}_2^\top\cdot\mathbf{a}_2^\perp = \mathbf{0}$, $\mathbf{A}_{0,1}^\top\cdot\mathbf{a}_{0,1}^\perp = \mathbf{0}$, $\mathbf{A}_{0,2}^\top\cdot\mathbf{a}_{0,2}^\perp = \mathbf{0}$) holds. For the convenience of our analysis, we sample $\widehat{sk} = \widehat{\mathbf{K}} \leftarrow_{\$} \mathbb{Z}_p^{\ell\times\ell}$ equivalently via

$$\widehat{sk} = \widehat{\mathbf{K}} := \widetilde{\mathbf{K}} + \mu_1\cdot\mathbf{a}_{0,2}^\perp\cdot(\mathbf{a}_1^\perp)^\top + \mu_2\cdot\mathbf{a}_2^\perp\cdot(\mathbf{a}_{0,1}^\perp)^\top \in \mathbb{Z}_p^{\ell\times\ell},$$

where $\widetilde{\mathbf{K}} \leftarrow_{\$} \mathbb{Z}_p^{\ell\times\ell}$ and $\mu_1,\mu_2 \leftarrow_{\$} \mathbb{Z}_p$. Consequently, we have

$$\widehat{pk}_\rho = \widehat{\alpha}_\rho(\widehat{sk}) = [\mathbf{A}_2]_2^\top\cdot\widehat{\mathbf{K}}\cdot[\mathbf{A}_1]_1 = [\mathbf{A}_2]_2^\top\cdot\widetilde{\mathbf{K}}\cdot[\mathbf{A}_1]_1,$$

$$\widehat{pk}_{\rho_0} = \widehat{\alpha}_{\rho_0}(\widehat{sk}) = [\mathbf{A}_{0,2}]_2^\top\cdot\widehat{\mathbf{K}}\cdot[\mathbf{A}_{0,1}]_1 = [\mathbf{A}_{0,2}]_2^\top\cdot\widetilde{\mathbf{K}}\cdot[\mathbf{A}_{0,1}]_1,$$

which may leak $\widetilde{\mathbf{K}}$, but μ_1 and μ_2 are completely hidden. Besides,

$$\begin{aligned}&\widehat{\Lambda}_{\widehat{sk}}([\mathbf{c}_1]_1,[\mathbf{c}_2]_2) = [\mathbf{c}_2]_2^\top\cdot\widehat{\mathbf{K}}\cdot[\mathbf{c}_1]_1\\ =\ &[\mathbf{c}_2]_2^\top\cdot\widetilde{\mathbf{K}}\cdot[\mathbf{c}_1]_1 + \boxed{\mu_1\cdot[\mathbf{c}_2^\top\mathbf{a}_{0,2}^\perp]_2\cdot[\mathbf{c}_1^\top\mathbf{a}_1^\perp]_1^\top} + \boxed{\mu_2\cdot[\mathbf{c}_2^\top\mathbf{a}_2^\perp]_2\cdot[\mathbf{c}_1^\top\mathbf{a}_{0,1}^\perp]_1^\top}.\end{aligned}$$

We divide the condition $([\mathbf{c}_1]_1,[\mathbf{c}_2]_2) \in \mathcal{X}\setminus(\mathcal{L}_\rho\cup\mathcal{L}_{\rho_0})$ into three cases:

– Case I: $[\mathbf{c}_1]_1 \in \mathsf{span}([\mathbf{A}_1]_1)$.

It must hold that $[\mathbf{c}_1]_1 \notin \mathsf{span}([\mathbf{A}_{0,1}]_1)$ and $[\mathbf{c}_2]_2 \notin \mathsf{span}([\mathbf{A}_2]_2)$: the former holds since $\mathsf{span}([\mathbf{A}_1]_1)\cap\mathsf{span}([\mathbf{A}_{0,1}]_1) = \emptyset$ (recall that the zero vector $[\mathbf{0}]_1$ is excluded from span spaces) and the latter is due to the fact that $([\mathbf{c}_1]_1,[\mathbf{c}_2]_2) \notin \mathcal{L}_\rho = \mathsf{span}([\mathbf{A}_1]_1)\times\mathsf{span}([\mathbf{A}_2]_2)$.

Thus, we can always find an $\mathbf{a}_2^\perp \in \mathbb{Z}_p^\ell$ such that $[\mathbf{c}_2^\top\mathbf{a}_2^\perp]_2 \neq [0]_2$ holds and find an $\mathbf{a}_{0,1}^\perp \in \mathbb{Z}_p^\ell$ such that $[\mathbf{c}_1^\top\mathbf{a}_{0,1}^\perp]_1 \neq [0]_1$ holds. Then, conditioned on $\widehat{pk}_\rho$ and $\widehat{pk}_{\rho_0}$, $\mu_2\cdot[\mathbf{c}_2^\top\mathbf{a}_2^\perp]_2\cdot[\mathbf{c}_1^\top\mathbf{a}_{0,1}^\perp]_1^\top$ is uniformly distributed over $\mathbb{G}_T$ due to the randomness of μ_2, so is $\widehat{\Lambda}_{\widehat{sk}}([\mathbf{c}_1]_1,[\mathbf{c}_2]_2)$.

– Case II: $[\mathbf{c}_2]_2 \in \mathsf{span}([\mathbf{A}_{0,2}]_2)$.

It must hold that $[\mathbf{c}_1]_1 \notin \mathsf{span}([\mathbf{A}_{0,1}]_1)$ and $[\mathbf{c}_2]_2 \notin \mathsf{span}([\mathbf{A}_2]_2)$: the former is due to the fact that $([\mathbf{c}_1]_1,[\mathbf{c}_2]_2) \notin \mathcal{L}_{\rho_0} = \mathsf{span}([\mathbf{A}_{0,1}]_1)\times\mathsf{span}([\mathbf{A}_{0,2}]_2)$ and the latter holds since $\mathsf{span}([\mathbf{A}_2]_2)\cap\mathsf{span}([\mathbf{A}_{0,2}]_2) = \emptyset$ (recall that the zero vector $[\mathbf{0}]_2$ is excluded from span spaces).

Similar to the analysis of Case I, conditioned on $\widehat{pk}_\rho$ and $\widehat{pk}_{\rho_0}$, $\widehat{\Lambda}_{\widehat{sk}}([\mathbf{c}_1]_1,[\mathbf{c}_2]_2)$ is uniformly distributed over $\mathbb{G}_T$.

– Case III: $[\mathbf{c}_1]_1 \notin \mathsf{span}([\mathbf{A}_1]_1)\ \wedge\ [\mathbf{c}_2]_2 \notin \mathsf{span}([\mathbf{A}_{0,2}]_2)$.

In this case, we can always find an $\mathbf{a}_1^\perp \in \mathbb{Z}_p^\ell$ such that $[\mathbf{c}_1^\top\mathbf{a}_1^\perp]_1 \neq [0]_1$ holds and find an $\mathbf{a}_{0,2}^\perp \in \mathbb{Z}_p^\ell$ such that $[\mathbf{c}_2^\top\mathbf{a}_{0,2}^\perp]_2 \neq [0]_2$ holds. Then, conditioned on $\widehat{pk}_\rho$ and $\widehat{pk}_{\rho_0}$, $\mu_1\cdot[\mathbf{c}_2^\top\mathbf{a}_{0,2}^\perp]_2\cdot[\mathbf{c}_1^\top\mathbf{a}_1^\perp]_1^\top$ is uniformly distributed over $\mathbb{G}_T$ due to the randomness of μ_1, so is $\widehat{\Lambda}_{\widehat{sk}}([\mathbf{c}_1]_1,[\mathbf{c}_2]_2)$.

In summary, $\widehat{\Lambda}_{\widehat{sk}}([\mathbf{c}_1]_1,[\mathbf{c}_2]_2)$ is uniformly distributed over $\mathbb{G}_T$ conditioned on $\widehat{pk}_\rho$ and $\widehat{pk}_{\rho_0}$ no matter which case it is.

This implies that $\widehat{\mathsf{QAHPS}}$ is perfectly $\langle\mathscr{L},\mathscr{L}_0\rangle$-universal.

[Perfectly $\langle\mathscr{L}_0,\mathscr{L}_1\rangle$-Universal.] It can be proved in a similar way as the perfectly $\langle\mathscr{L},\mathscr{L}_0\rangle$-universal.

[κ-LR-$\langle\mathscr{L},\mathscr{L}_0\rangle$-Universal.] It follows from Lemma 7.

[κ-LR-$\langle\mathscr{L},\mathscr{L}_0\rangle$-Key-Switching.] Let $(\rho = ([\mathbf{A}_1]_1,[\mathbf{A}_2]_2) \in \mathbb{G}_1^{\ell\times k}\times\mathbb{G}_2^{\ell\times k},\ td) \leftarrow_{\$} \mathscr{L}$ and let $L : \widehat{\mathcal{SK}} \longrightarrow \{0,1\}^\kappa$ be an arbitrary leakage function. For $\widehat{sk} = \widehat{\mathbf{K}} \leftarrow_{\$} \mathbb{Z}_p^{\ell\times\ell}$, $\widehat{sk}' = \widehat{\mathbf{K}'} \leftarrow_{\$} \mathbb{Z}_p^{\ell\times\ell}$ and

$(\rho_0 = ([\mathbf{A}_{0,1}]_1, [\mathbf{A}_{0,2}]_2) \in \mathbb{G}_1^{\ell \times k} \times \mathbb{G}_2^{\ell \times k},\ td_0) \leftarrow_{\$} \mathscr{L}_0$, we aim to prove

$$\varDelta\Big(\big(\rho_0, \underbrace{\boxed{[\mathbf{A}_{0,2}]_2^\top \widehat{\mathbf{K}} [\mathbf{A}_{0,1}]_1}}_{\widehat{\alpha}_{\rho_0}(\widehat{sk})}\big), \big(\rho_0, \underbrace{\boxed{[\mathbf{A}_{0,2}]_2^\top \widehat{\mathbf{K}'} [\mathbf{A}_{0,1}]_1}}_{\widehat{\alpha}_{\rho_0}(\widehat{sk'})}\big) \ \Big|\ \underbrace{[\mathbf{A}_2]_2^\top \widehat{\mathbf{K}} [\mathbf{A}_1]_1}_{\widehat{\alpha}_{\rho}(\widehat{sk})},\ L(\widehat{\mathbf{K}}) \Big) \leq 2^{-\Omega(\lambda)}. \quad (15)$$

Taking $[\mathbf{A}_{0,1}]_1$ as a universal hash function and the ℓ rows of $\widehat{\mathbf{K}}$ as ℓ independent inputs, we have that

$$\varDelta\Big(\big([\mathbf{A}_{0,1}]_1, \widehat{\mathbf{K}}[\mathbf{A}_{0,1}]_1\big), \big([\mathbf{A}_{0,1}]_1, [\mathbf{U}]_1\big) \ \Big|\ \widehat{\mathbf{K}}[\mathbf{A}_1]_1,\ L(\widehat{\mathbf{K}}) \Big) \ \leq\ 2^{-\Omega(\lambda)}, \quad (16)$$

where $\mathbf{U} \leftarrow_{\$} \mathbb{Z}_p^{\ell \times k}$, by the multi-fold generalized leftover hash lemma (i.e., Lemma 4 in Subsect. 2.1). Meanwhile, $\widehat{\mathbf{K}'}$ is uniform and independent of $\mathbf{A}_{0,1}, \mathbf{A}_1$ and $\widehat{\mathbf{K}}$. So,

$$\big([\mathbf{A}_{0,1}]_1, \boxed{[\mathbf{U}]_1}, \widehat{\mathbf{K}}[\mathbf{A}_1]_1,\ L(\widehat{\mathbf{K}}) \big) \equiv \big([\mathbf{A}_{0,1}]_1, \boxed{\widehat{\mathbf{K}'}[\mathbf{A}_{0,1}]_1}, \widehat{\mathbf{K}}[\mathbf{A}_1]_1,\ L(\widehat{\mathbf{K}}) \big). \quad (17)$$

(16) and (17) implies

$$\varDelta\Big(\big([\mathbf{A}_{0,1}]_1, \boxed{\widehat{\mathbf{K}}[\mathbf{A}_{0,1}]_1}\big), \big([\mathbf{A}_{0,1}]_1, \boxed{\widehat{\mathbf{K}'}[\mathbf{A}_{0,1}]_1}\big) \ \Big|\ \widehat{\mathbf{K}}[\mathbf{A}_1]_1,\ L(\widehat{\mathbf{K}}) \Big) \ \leq\ 2^{-\Omega(\lambda)}. \quad (18)$$

Note that the variables in $\varDelta()$ of (15) can be regarded as outputs of certain randomized function of the variables in $\varDelta()$ of (18). By Lemma 2, (15) holds.

This completes the proof of κ-LR-$\langle \mathscr{L}, \mathscr{L}_0 \rangle$-key-switching. □

5.5 The Instantiation of LR-Weak-Ardent Tag-Based QAHPS

We present the construction of tag-based $\widetilde{\mathsf{QAHPS}} = (\widetilde{\mathsf{Setup}}, \widetilde{\alpha}_{(\cdot)}, \widetilde{\mathsf{Pub}}, \widetilde{\mathsf{Priv}})$ for the language distribution $\mathscr{L}$ $(= \mathscr{L}_{\mathcal{D}_{\ell,k}})$ in Fig. 5. It is straightforward to check the perfect correctness of $\widetilde{\mathsf{QAHPS}}$.

$\widetilde{pp} \leftarrow_{\$} \widetilde{\mathsf{Setup}}(1^\lambda)$: $\mathcal{PG} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, e, P_1, P_2, P_T) \leftarrow_{\$} \mathsf{PGGen}(1^\lambda)$. $\Rightarrow \widetilde{pp} := \mathcal{PG}$, which implicitly defines $(\widetilde{\mathcal{SK}} := \mathbb{Z}_p^{2 \times \ell},\ \widetilde{\mathcal{T}} := \mathbb{G}_2,\ \widetilde{\Pi} := \mathbb{G}_T,\ \widetilde{\Lambda}_{(\cdot)})$, where $\widetilde{\Lambda}_{\widetilde{sk}}(([\mathbf{c}_1]_1, [\mathbf{c}_2]_2), [\tau]_2) := [1, \tau]_2 \cdot \widetilde{\mathbf{K}} \cdot [\mathbf{c}_1]_1 \in \mathbb{G}_T$ for any $\widetilde{sk} = \widetilde{\mathbf{K}} \in \mathbb{Z}_p^{2 \times \ell}$, $([\mathbf{c}_1]_1, [\mathbf{c}_2]_2) \in \mathcal{X} = \mathbb{G}_1^\ell \times \mathbb{G}_2^\ell$ and $[\tau]_2 \in \mathbb{G}_2$.	$\widetilde{pk}_\rho \leftarrow \widetilde{\alpha}_\rho(\widetilde{sk})$, where $\rho = ([\mathbf{A}_1]_1, [\mathbf{A}_2]_2) \in \mathbb{G}_1^{\ell \times k} \times \mathbb{G}_2^{\ell \times k}$: Parse $\widetilde{sk} = \widetilde{\mathbf{K}} \in \mathbb{Z}_p^{2 \times \ell}$. $[\widetilde{\mathbf{P}}]_1 := \widetilde{\mathbf{K}} \cdot [\mathbf{A}_1]_1 \in \mathbb{G}_1^{2 \times k}$. $\Rightarrow \widetilde{pk}_\rho := [\widetilde{\mathbf{P}}]_1$.
$[\widetilde{\pi}]_T \leftarrow \widetilde{\mathsf{Pub}}(\widetilde{pk}_\rho, ([\mathbf{c}_1]_1, [\mathbf{c}_2]_2), (\mathbf{w}_1, \mathbf{w}_2) \in \mathbb{Z}_p^k \times \mathbb{Z}_p^k, [\tau]_2 \in \mathbb{G}_2)$, where $([\mathbf{c}_1]_1, [\mathbf{c}_2]_2) \in \mathcal{L}_\rho$ for $\rho = ([\mathbf{A}_1]_1, [\mathbf{A}_2]_2)$: Parse $\widetilde{pk}_\rho = [\widetilde{\mathbf{P}}]_1 \in \mathbb{G}_1^{2 \times k}$. $\Rightarrow [\widetilde{\pi}]_T := [1, \tau]_2 \cdot [\widetilde{\mathbf{P}}]_1 \cdot \mathbf{w}_1 \in \mathbb{G}_T$.	$[\widetilde{\pi}]_T \leftarrow \widetilde{\mathsf{Priv}}(\widetilde{sk}, ([\mathbf{c}_1]_1, [\mathbf{c}_2]_2) \in \mathcal{X}, [\tau]_2)$: Parse $\widetilde{sk} = \widetilde{\mathbf{K}} \in \mathbb{Z}_p^{2 \times \ell}$. $\Rightarrow [\widetilde{\pi}]_T := [1, \tau]_2 \cdot \widetilde{\mathbf{K}} \cdot [\mathbf{c}_1]_1 \in \mathbb{G}_T$.

Fig. 5. Construction of LR-weak-ardent tag-based $\widetilde{\mathsf{QAHPS}}$ over asymmetric pairing groups.

Theorem 5 (LR-weak-ardency of Tag-Based $\widetilde{\mathsf{QAHPS}}$). *Let $\ell \geq 2k+1$ and $\kappa \leq \log p - \Omega(\lambda)$. The proposed tag-based $\widetilde{\mathsf{QAHPS}}$ scheme for $\mathscr{L}$ in Fig. 5 satisfies the properties listed in Table 2, i.e., (1) it is $\langle \perp, \perp \rangle$-universal and (2) it supports κ-LR-$\langle \mathscr{L}, \mathscr{L}_0 \rangle$- and $\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-key-switching, where $\mathscr{L} = \mathscr{L}_{\mathcal{D}_{\ell,k}}$, $\mathscr{L}_0 = \mathscr{L}_{\mathcal{U}_{\ell,k}}$ and $\mathscr{L}_1 = \mathscr{L}_{\mathcal{U}'_{\ell,k}}$ are specified in Subsect. 5.2.*

Proof of Theorem 5.

[(Perfectly) $\langle\perp,\perp\rangle$-Universal.] For $\widetilde{sk} = \widetilde{\mathbf{K}} \leftarrow_{\$} \mathbb{Z}_p^{2\times\ell}$, any $([\mathbf{c}_1]_1, [\mathbf{c}_2]_2) \in \mathcal{X} \setminus \mathcal{L}_{\rho_\perp} = \mathcal{X}$, any $([\mathbf{c}'_1]_1, [\mathbf{c}'_2]_2) \in \mathcal{X}$ and any $[\tau]_2, [\tau']_2 \in \mathbb{G}_2$ with $[\tau]_2 \neq [\tau']_2$, we consider the distribution of $\widetilde{\Lambda}_{\widetilde{sk}}(([\mathbf{c}_1]_1, [\mathbf{c}_2]_2), [\tau]_2)$ conditioned on $\widetilde{\Lambda}_{\widetilde{sk}}(([\mathbf{c}'_1]_1, [\mathbf{c}'_2]_2), [\tau']_2)$.

Observe that $[1, \tau']_2$ is linearly independent of $[1, \tau]_2$ when $[\tau]_2 \neq [\tau']_2$, thus we can always find a vector $\mathbf{a} = \binom{\tau'}{-1} \in \mathbb{Z}_p^2$ orthogonal to $[1, \tau']_2$ but non-orthogonal to $[1, \tau]_2$, i.e., $[1, \tau']_2 \cdot \mathbf{a} = [0]_2$ but $[1, \tau]_2 \cdot \mathbf{a} \neq [0]_2$. For convenience, we sample $\widetilde{sk} = \widetilde{\mathbf{K}} \leftarrow_{\$} \mathbb{Z}_p^{2\times\ell}$ equivalently via

$$\widetilde{sk} = \widetilde{\mathbf{K}} := \overline{\mathbf{K}} + \mathbf{a} \cdot \overline{\mathbf{k}}^\top \in \mathbb{Z}_p^{2\times\ell},$$

where $\overline{\mathbf{K}} \leftarrow_{\$} \mathbb{Z}_p^{2\times\ell}$ and $\overline{\mathbf{k}} \leftarrow_{\$} \mathbb{Z}_p^{\ell}$. Consequently, we have

$$\widetilde{\Lambda}_{\widetilde{sk}}(([\mathbf{c}'_1]_1, [\mathbf{c}'_2]_2), [\tau']_2) = [1, \tau']_2 \cdot \widetilde{\mathbf{K}} \cdot [\mathbf{c}'_1]_1 = [1, \tau']_2 \cdot \overline{\mathbf{K}} \cdot [\mathbf{c}'_1]_1,$$

which may leak $\overline{\mathbf{K}}$, but the value of $\overline{\mathbf{k}}$ is perfectly hidden. Besides,

$$\widetilde{\Lambda}_{\widetilde{sk}}(([\mathbf{c}_1]_1, [\mathbf{c}_2]_2), [\tau]_2) = [1, \tau]_2 \cdot \widetilde{\mathbf{K}} \cdot [\mathbf{c}_1]_1 = [1, \tau]_2 \cdot \overline{\mathbf{K}} \cdot [\mathbf{c}_1]_1 + \boxed{[1, \tau]_2 \cdot \mathbf{a} \cdot \overline{\mathbf{k}}^\top \cdot [\mathbf{c}_1]_1}.$$

Since $([\mathbf{c}_1]_1, [\mathbf{c}_2]_2) \neq ([\mathbf{0}]_1, [\mathbf{0}]_2)$ (recall that $([\mathbf{0}]_1, [\mathbf{0}]_2)$ is excluded from $\mathcal{X}$), $\overline{\mathbf{k}}^\top \cdot [\mathbf{c}_1]_1$ is uniformly distributed over $\mathbb{G}_1$ conditioned on $\widetilde{\Lambda}_{\widetilde{sk}}(([\mathbf{c}'_1]_1, [\mathbf{c}'_2]_2), [\tau']_2)$, due to the randomness of $\overline{\mathbf{k}}$. Together with the fact that $[1, \tau]_2 \cdot \mathbf{a} \neq [0]$, $[1, \tau]_2 \cdot \mathbf{a} \cdot \overline{\mathbf{k}}^\top \cdot [\mathbf{c}_1]_1$ is uniformly distributed over $\mathbb{G}_T$ conditioned on $\widetilde{\Lambda}_{\widetilde{sk}}(([\mathbf{c}'_1]_1, [\mathbf{c}'_2]_2), [\tau']_2)$, and so is $\widetilde{\Lambda}_{\widetilde{sk}}(([\mathbf{c}_1]_1, [\mathbf{c}_2]_2), [\tau]_2)$. Hence

$$\widetilde{\mathbf{H}}_\infty\big(\widetilde{\Lambda}_{\widetilde{sk}}(([\mathbf{c}_1]_1, [\mathbf{c}_2]_2), [\tau]_2) \mid \widetilde{\Lambda}_{\widetilde{sk}}(([\mathbf{c}'_1]_1, [\mathbf{c}'_2]_2), [\tau']_2)\big) = \log p \geq \Omega(\lambda).$$

This implies that $\widetilde{\mathsf{QAHPS}}$ is (perfectly) $\langle\perp,\perp\rangle$-universal.

[κ-LR-$\langle\mathscr{L}, \mathscr{L}_0\rangle$-Key-Switching.] The proof is a simplified version of that for $\widehat{\mathsf{QAHPS}}$ (cf. Theorem 4). In fact, (16), (17) and (18) suffice for the proof.

[$\langle\mathscr{L}_0, \mathscr{L}_1\rangle$-Key-Switching.] $\langle\mathscr{L}_0, \mathscr{L}_1\rangle$-key-switching is proved similarly. □

5.6 Tightly LR-CCA-Secure PKE over Asymmetric Pairing Groups

We are able to instantiate (the more efficient variant of) our generic construction of LR-CCA secure PKE in Sect. 4 (cf. Remark 8 and Fig. 15 in Appendix D) with the LR-weak-ardent QAHPS (cf. Fig. 3), the LR-ardent $\widehat{\mathsf{QAHPS}}$ (cf. Fig. 4) and the LR-weak-ardent tag-based $\widetilde{\mathsf{QAHPS}}$ (cf. Fig. 5) over asymmetric pairing groups $\mathcal{PG} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, e, P_1, P_2, P_T)$ based on the $\mathcal{D}_{\ell,k}$-MDDH assumptions. Let $\mathcal{H} = \{\mathsf{H} : \mathbb{G}_1^\ell \times \mathbb{G}_2^{\ell+1} \longrightarrow \mathbb{G}_2\}$ be a collision-resistant function family. We present the instantiation $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{asym}}$ with message space $\mathcal{M} = \mathbb{G}_2$ in Fig. 6. The scheme can be easily extended to encrypt vectors over $\mathbb{G}_2$, by replacing the vector $\mathbf{k}$ in the secret key with a matrix.

For $\ell \geq 2k+1$ and $\kappa \leq \log p - \Omega(\lambda)$, by combining Theorem 1, Lemma 9 and Theorems 2, 3, 4, 5 together, we obtain the following corollary regarding the LR-CCA security of our instantiation $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{asym}}$.

Corollary 1 (LR-CCA Security of $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{asym}}$). *Let $\ell \geq 2k+1$ and $\kappa \leq \log p - \Omega(\lambda)$. If (i) the $\mathcal{D}_{\ell,k}$-MDDH assumption holds over both $\mathbb{G}_1$ and $\mathbb{G}_2$, (ii) $\mathcal{H}$ is a collision-resistant function family, then the instantiation $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{asym}}$ in Fig. 6 is κ-LR-CCA secure. Concretely, for any adversary $\mathcal{A}$ who makes at most Q_e times of* Enc *queries and Q_d times of* Dec *queries, there exist adversaries $\mathcal{B}_1$, $\mathcal{B}_2$ and $\mathcal{B}_3$, such that $\mathbf{T}(\mathcal{B}_3) \approx \mathbf{T}(\mathcal{A}) + (Q_e + Q_d) \cdot \mathsf{poly}(\lambda)$, $\mathbf{T}(\mathcal{B}_1) \approx \mathbf{T}(\mathcal{B}_2) \approx \mathbf{T}(\mathcal{A}) + (Q_e + Q_e \cdot Q_d) \cdot \mathsf{poly}(\lambda)$, with $\mathsf{poly}(\lambda)$ independent of $\mathbf{T}(\mathcal{A})$, and*

$$\begin{aligned}\mathsf{Adv}^{\kappa\text{-}lr\text{-}cca}_{\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{asym}},\mathcal{A}}(\lambda) \leq{}& (4\lceil\log Q_e\rceil + \ell - k + 2) \cdot \big(\mathsf{Adv}^{mddh}_{\mathcal{D}_{\ell,k},\mathbb{G}_1,\mathcal{B}_1}(\lambda) + \mathsf{Adv}^{mddh}_{\mathcal{D}_{\ell,k},\mathbb{G}_2,\mathcal{B}_2}(\lambda)\big) \\ &+ \mathsf{Adv}^{cr}_{\mathcal{H},\mathcal{B}_3}(\lambda) + (4 + Q_d + Q_d Q_e + \lceil\log Q_e\rceil \cdot (Q_d + Q_e + Q_d Q_e)) \cdot 2^{-\Omega(\lambda)}.\end{aligned}$$

$\underline{\mathsf{PP} \leftarrow_\$ \mathsf{Param}(1^\lambda):}$

$\mathcal{PG} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, e, P_1, P_2, P_T) \leftarrow_\$ \mathsf{PGGen}(1^\lambda)$.

$\mathbf{A}_1, \mathbf{A}_2 \leftarrow_\$ \mathcal{D}_{\ell,k}$. $\quad \mathsf{H} \leftarrow_\$ \mathcal{H}$.

$\Rightarrow \mathsf{PP} := (\mathcal{PG}, [\mathbf{A}_1]_1, [\mathbf{A}_2]_2, \mathsf{H})$.

$\underline{C \leftarrow_\$ \mathsf{Enc}(\mathsf{PK}, [M]_2 \in \mathbb{G}_2):}$

$\mathbf{w}_1 \leftarrow_\$ \mathbb{Z}_p^k$. $\quad [\mathbf{c}_1]_1 := [\mathbf{A}_1]_1 \cdot \mathbf{w}_1 \in \mathbb{G}_1^\ell$.

$\mathbf{w}_2 \leftarrow_\$ \mathbb{Z}_p^k$. $\quad [\mathbf{c}_2]_2 := [\mathbf{A}_2]_2 \cdot \mathbf{w}_2 \in \mathbb{G}_2^\ell$.

$[d]_2 := [\mathbf{p}^\top]_2 \cdot \mathbf{w}_2 + [M]_2 \in \mathbb{G}_2$.

$[\tau]_2 := \mathsf{H}([\mathbf{c}_1]_1, [\mathbf{c}_2]_2, [d]_2) \in \mathbb{G}_2$.

$[\pi]_T := \underbrace{\mathbf{w}_2^\top \cdot [\widehat{\mathbf{P}}]_T \cdot \mathbf{w}_1}_{[\widehat{\pi}]_T} + \underbrace{[1, \tau]_2 \cdot [\widetilde{\mathbf{P}}]_1 \cdot \mathbf{w}_1}_{[\widetilde{\pi}]_T} \in \mathbb{G}_T$.

$\Rightarrow C := ([\mathbf{c}_1]_1, [\mathbf{c}_2]_2, [d]_2, [\pi]_T) \in \mathbb{G}_1^\ell \times \mathbb{G}_2^{\ell+1} \times \mathbb{G}_T$.

$\underline{(\mathsf{PK}, \mathsf{SK}) \leftarrow_\$ \mathsf{Gen}(\mathsf{PP}):}$

$\mathbf{k} \leftarrow_\$ \mathbb{Z}_p^\ell$. $\quad [\mathbf{p}^\top]_2 := \mathbf{k}^\top \cdot [\mathbf{A}_2]_2 \in \mathbb{G}_2^{1 \times k}$.

$\widehat{\mathbf{K}} \leftarrow_\$ \mathbb{Z}_p^{\ell \times \ell}$. $\quad [\widehat{\mathbf{P}}]_T := [\mathbf{A}_2]_2^\top \cdot \widehat{\mathbf{K}} \cdot [\mathbf{A}_1]_1 \in \mathbb{G}_T^{k \times k}$.

$\widetilde{\mathbf{K}} \leftarrow_\$ \mathbb{Z}_p^{2 \times \ell}$. $\quad [\widetilde{\mathbf{P}}]_1 := \widetilde{\mathbf{K}} \cdot [\mathbf{A}_1]_1 \in \mathbb{G}_1^{2 \times k}$.

$\Rightarrow \mathsf{PK} := ([\mathbf{p}]_2, [\widehat{\mathbf{P}}]_T, [\widetilde{\mathbf{P}}]_1)$, $\quad \mathsf{SK} := (\mathbf{k}, \widehat{\mathbf{K}}, \widetilde{\mathbf{K}})$.

$\underline{[M]_2 / \perp \leftarrow \mathsf{Dec}(\mathsf{SK}, C):}$

Parse $C = ([\mathbf{c}_1]_1, [\mathbf{c}_2]_2, [d]_2, [\pi']_T)$.

$[M]_2 := [d]_2 - \mathbf{k}^\top \cdot [\mathbf{c}_2]_2 \in \mathbb{G}_2$.

$[\tau]_2 := \mathsf{H}([\mathbf{c}_1]_1, [\mathbf{c}_2]_2, [d]_2) \in \mathbb{G}_2$.

$[\pi]_T := \underbrace{[\mathbf{c}_2]_2^\top \cdot \widehat{\mathbf{K}} \cdot [\mathbf{c}_1]_1}_{[\widehat{\pi}]_T} + \underbrace{[1, \tau]_2 \cdot \widetilde{\mathbf{K}} \cdot [\mathbf{c}_1]_1}_{[\widetilde{\pi}]_T} \in \mathbb{G}_T$.

$\Rightarrow$ If $[\pi']_T = [\pi]_T$, Return $[M]_2 \in \mathbb{G}_2$;

Else, Return $\perp$.

Fig. 6. The instantiation $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{asym}}$ over asymmetric pairing groups. The message space is $\mathcal{M} = \mathbb{G}_2$. Here $\mathcal{H} = \{\mathsf{H} : \mathbb{G}_1^\ell \times \mathbb{G}_2^{\ell+1} \longrightarrow \mathbb{G}_2\}$ is a collision-resistant function family.

Tight LR-CCA Security, Efficiency and Leakage-Rate of $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{asym}}$. When $\mathcal{D}_{\ell,k} := \mathcal{U}_{\ell,k}$, the LR-CCA security of $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{asym}}$ is tightly reduced to the standard k-LIN assumption since k-LIN implies $\mathcal{U}_{\ell,k}$-MDDH by Lemma 5. Let $k\mathbb{G}$ denote k elements in $\mathbb{G}$. By taking $\ell = 2k+1$, we have $\mathsf{PP} : (2k^2+k)\mathbb{G}_1 + (2k^2+k)\mathbb{G}_2$, $\mathsf{PK} : 2k\mathbb{G}_1 + k\mathbb{G}_2 + k^2\mathbb{G}_T$, $\mathsf{SK} : (4k^2+10k+4)\mathbb{Z}_p$, and $C : (2k+1)\mathbb{G}_1 + (2k+2)\mathbb{G}_2 + 1\mathbb{G}_T$. See Table 1 for details. Furthermore, if we choose $\kappa = \log p - \Omega(\lambda)$, then the leakage-rate of the LR-CCA security is $\kappa / \mathsf{BitLength}(\mathsf{SK}) = \frac{1}{4k^2+10k+4} \cdot (1 - \frac{\Omega(\lambda)}{\log p})$, which is arbitrarily close to $1/(4k^2+10k+4)$ if we choose a sufficiently large p.

Particularly, in case $k = 1$, the tight LR-CCA security of $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{asym}}$ is based on the SXDH assumption and it has $\mathsf{PK} : 2\mathbb{G}_1 + 1\mathbb{G}_2 + 1\mathbb{G}_T$, $C : 3\mathbb{G}_1 + 4\mathbb{G}_2 + 1\mathbb{G}_T$ and leakage-rate $= 1/18 - o(1)$.

Remark 10 (Tight LR-CCA Security in the Multi-User Setting). For better readability, we merely considered the LR-CCA security in the single-user setting so far. Our results extend naturally to the multi-user setting. (The definition of LR-CCA security in the multi-user setting is presented in Appendix A.1.) In our single-user LR-CCA security proof (i.e., the proof of Theorem 1), most steps are statistical arguments (e.g., using the LR-universal or LR-key-switching properties of the underlying QAHPS schemes), thus could be easily carried over to the multi-user setting. The only points that are not statistical and hence need to be adapted is the use of the SMP assumptions (e.g., the game transition $\mathsf{G}_2 \to \mathsf{G}_3$ in the proof of Theorem 1) and the multi-extracting property (the game transition $\mathsf{G}_5 \to \mathsf{G}_6$). The adaptions are straightforward: the former is essentially unchanged, since the language parameter ρ that the SMP is w.r.t. is part of the public parameters PP, shared by all users; the latter could be tightly reduced to the MDDH assumptions for multiple users, by the random self-reducibility of MDDH.

6 Instantiations over Symmetric Pairing Groups

In this section, we instantiate our generic construction of LR-CCA secure PKE in Sect. 4 over symmetric pairing groups and obtain a PKE scheme $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{sym}}$. This is essentially a simplification of the instantiations over asymmetric pairing groups shown in Sect. 5.

6.1 The Language Distribution for Linear Subspaces

Let $\mathcal{PG} = (\mathbb{G}, \mathbb{G}_T, p, e, P, P_T)$ be a symmetric pairing group. For any matrix distribution $\mathcal{D}_{\ell,k}$, which outputs matrices in $\mathbb{Z}_p^{\ell \times k}$, it naturally gives rise to a language distribution $\mathscr{L}_{\mathcal{D}_{\ell,k}}$ for linear subspaces over group $\mathbb{G}$:

– $\mathscr{L}_{\mathcal{D}_{\ell,k}}$ invokes $\mathbf{A} \leftarrow_\$ \mathcal{D}_{\ell,k}$, and outputs a language parameter $\rho = [\mathbf{A}] \in \mathbb{G}^{\ell \times k}$ together with a trapdoor $td = \mathbf{A} \in \mathbb{Z}_p^{\ell \times k}$.

The matrix ρ defines a linear subspace language $\mathcal{L}_\rho$ on $\mathbb{G}^\ell$:

$$\mathcal{L}_\rho = \mathsf{span}([\mathbf{A}]) = \left\{ [\mathbf{c}] \mid \exists\, \mathbf{w} \in \mathbb{Z}_p^k \setminus \{\mathbf{0}\},\ \text{s.t. } [\mathbf{c}] = [\mathbf{A}\mathbf{w}] \right\} \subseteq \mathcal{X} = \mathbb{G}^\ell \setminus \{[\mathbf{0}]\}.^{9}$$

The trapdoor td can be used to decide whether or not an instance $[\mathbf{c}]$ is in $\mathcal{L}_\rho$ efficiently: first compute a basis of the kernel space of $\mathbf{A}^\top$, namely $\mathbf{A}^\perp \in \mathbb{Z}_p^{\ell \times (\ell-k)}$ satisfying $\mathbf{A}^\top \cdot \mathbf{A}^\perp = \mathbf{0}$, then check whether $[\mathbf{c}^\top \cdot \mathbf{A}^\perp] = [\mathbf{0}]$ holds.

Clearly, the SMP related to $\mathscr{L}_{\mathcal{D}_{\ell,k}}$ corresponds to the $\mathcal{D}_{\ell,k}$-MDDH over group $\mathbb{G}$, and the multi-fold SMP related to $\mathscr{L}_{\mathcal{D}_{\ell,k}}$ corresponds to the Q-fold $\mathcal{D}_{\ell,k}$-MDDH over $\mathbb{G}$ for any $Q = \mathsf{poly}(\lambda)$. The same also holds for the uniform distribution $\mathcal{U}_{\ell,k}$. Formally, we have the following lemma, which is a corollary of the random self-reducibility of $\mathcal{D}_{\ell,k}$-MDDH and $\mathcal{U}_{\ell,k}$-MDDH (i.e., Lemma 6).

Lemma 10 ($\mathcal{D}_{\ell,k}/\mathcal{U}_{\ell,k}$-MDDH $\Rightarrow$ Multi-fold SMP related to $\mathscr{L}_{\mathcal{D}_{\ell,k}}/\mathscr{L}_{\mathcal{U}_{\ell,k}}$). *Let $Q > \ell - k$. For any adversary $\mathcal{A}$, there exists an adversary $\mathcal{B}$, such that $\mathbf{T}(\mathcal{B}) \approx \mathbf{T}(\mathcal{A}) + Q \cdot \mathsf{poly}(\lambda)$ with $\mathsf{poly}(\lambda)$ independent of $\mathbf{T}(\mathcal{A})$, and*

$$\mathsf{Adv}^{Q\text{-}msmp}_{\mathscr{L}_{\mathcal{D}_{\ell,k}},\mathcal{A}}(\lambda) \le (\ell - k) \cdot \mathsf{Adv}^{mddh}_{\mathcal{D}_{\ell,k},\mathbb{G},\mathcal{B}}(\lambda) + 1/(p-1).$$

For any adversary $\mathcal{A}$, there exists an adversary $\mathcal{B}$, such that $\mathbf{T}(\mathcal{B}) \approx \mathbf{T}(\mathcal{A}) + Q \cdot \mathsf{poly}(\lambda)$ with $\mathsf{poly}(\lambda)$ independent of $\mathbf{T}(\mathcal{A})$, and

$$\mathsf{Adv}^{Q\text{-}msmp}_{\mathscr{L}_{\mathcal{U}_{\ell,k}},\mathcal{A}}(\lambda) \le \mathsf{Adv}^{mddh}_{\mathcal{U}_{\ell,k},\mathbb{G},\mathcal{B}}(\lambda) + 1/(p-1).$$

6.2 The Instantiation of Language Distributions

To instantiate the generic PKE construction in Sect. 4, the first thing we need to do is to determine three language distributions $\mathscr{L}$, $\mathscr{L}_0$ and $\mathscr{L}_1$ carefully.

Let $\ell \ge 2k+1$. Let $\mathcal{D}_{\ell,k}$ be an (arbitrary) matrix distribution, and $\mathcal{U}_{\ell,k}$, $\mathcal{U}'_{\ell,k}$ independent copies of the uniform distribution, all of which output matrices in $\mathbb{Z}_p^{\ell \times k}$. Based on the previous subsection, we designate the language distributions $\mathscr{L}$, $\mathscr{L}_0$ and $\mathscr{L}_1$ as follows.

- $\mathscr{L} := \mathscr{L}_{\mathcal{D}_{\ell,k}}$, which invokes $\mathbf{A} \leftarrow_\$ \mathcal{D}_{\ell,k}$ and outputs $(\rho = [\mathbf{A}], td = \mathbf{A})$;
- $\mathscr{L}_0 := \mathscr{L}_{\mathcal{U}_{\ell,k}}$, which invokes $\mathbf{A}_0 \leftarrow_\$ \mathcal{U}_{\ell,k}$ and outputs $(\rho_0 = [\mathbf{A}_0], td_0 = \mathbf{A}_0)$;
- $\mathscr{L}_1 := \mathscr{L}_{\mathcal{U}'_{\ell,k}}$, which invokes $\mathbf{A}_1 \leftarrow_\$ \mathcal{U}'_{\ell,k}$ and outputs $(\rho_1 = [\mathbf{A}_1], td_1 = \mathbf{A}_1)$.

6.3 The Instantiation of LR-Weak-Ardent QAHPS

We present the construction of $\mathsf{QAHPS} = (\mathsf{Setup}, \alpha_{(\cdot)}, \mathsf{Pub}, \mathsf{Priv})$ for the language distribution $\mathscr{L}$ $(= \mathscr{L}_{\mathcal{D}_{\ell,k}})$ in Fig. 7. It is straightforward to check the perfect correctness of QAHPS: for all language parameters $\rho = [\mathbf{A}] \in \mathbb{G}^{\ell \times k}$, all $sk = \mathbf{k} \in \mathbb{Z}_p^\ell$ and $pk_\rho = \alpha_\rho(sk) = [\mathbf{p}^\top] = \mathbf{k}^\top \cdot [\mathbf{A}] \in \mathbb{G}^{1 \times k}$, all $[\mathbf{c}] = [\mathbf{A}\mathbf{w}] \in \mathcal{L}_\rho$ with witness $\mathbf{w} \in \mathbb{Z}_p^k$, it follows that $\mathsf{Pub}(pk_\rho, [\mathbf{c}], \mathbf{w}) = [\mathbf{p}^\top] \cdot \mathbf{w} = \mathbf{k}^\top \cdot [\mathbf{A}\mathbf{w}] = \mathsf{Priv}(sk, [\mathbf{c}])$.

Theorem 6 ($\mathscr{L}_0$-Multi-Extracting of QAHPS). *If the $\mathcal{U}_{k+1,k}$-MDDH assumption holds over $\mathbb{G}$, then the proposed QAHPS in Fig. 7 is $\mathscr{L}_0$-multi-extracting, where the language distribution $\mathscr{L}_0$ $(= \mathscr{L}_{\mathcal{U}_{\ell,k}})$ is specified in Subsect. 6.2.*

Concretely, for any adversary $\mathcal{A}$, any polynomial $Q = \mathsf{poly}(\lambda)$, there exists an adversary $\mathcal{B}$, such that $\mathbf{T}(\mathcal{B}) \approx \mathbf{T}(\mathcal{A}) + Q \cdot \mathsf{poly}(\lambda)$ with $\mathsf{poly}(\lambda)$ independent of $\mathbf{T}(\mathcal{A})$, and

$$\mathsf{Adv}^{Q\text{-}\mathscr{L}_0\text{-}mext}_{\mathsf{QAHPS},\mathcal{A}}(\lambda) \le \mathsf{Adv}^{mddh}_{\mathcal{U}_{k+1,k},\mathbb{G},\mathcal{B}}(\lambda) + 1/(p-1).$$

[9] For technical reasons, the zero vector $[\mathbf{0}]$ must be excluded from both $\mathcal{L}_\rho$ and $\mathcal{X}$. For the sake of simplicity, we forgo making this explicit in the sequel.

$\underline{pp \leftarrow_{\$} \mathsf{Setup}(1^\lambda)}$: $\mathcal{PG} = (\mathbb{G}, \mathbb{G}_T, p, e, P, P_T) \leftarrow_{\$} \mathsf{PGGen}(1^\lambda)$. $\Rightarrow pp := \mathcal{PG}$, which implicitly defines $(\mathcal{SK} := \mathbb{Z}_p^\ell,\ \Pi := \mathbb{G},\ \Lambda_{(\cdot)})$, where $\Lambda_{sk}([\mathbf{c}]) := \mathbf{k}^\top \cdot [\mathbf{c}] \in \mathbb{G}$ for any $sk = \mathbf{k} \in \mathbb{Z}_p^\ell$ and $[\mathbf{c}] \in \mathcal{X} = \mathbb{G}^\ell$.	$pk_\rho \leftarrow \alpha_\rho(sk)$, where $\rho = [\mathbf{A}] \in \mathbb{G}^{\ell \times k}$: Parse $sk = \mathbf{k} \in \mathbb{Z}_p^\ell$. $[\mathbf{p}^\top] := \mathbf{k}^\top \cdot [\mathbf{A}] \in \mathbb{G}^{1 \times k}$. $\Rightarrow pk_\rho := [\mathbf{p}^\top]$.
$[\pi] \leftarrow \mathsf{Pub}(pk_\rho, [\mathbf{c}] \in \mathbb{G}^\ell, \mathbf{w} \in \mathbb{Z}_p^k)$, where $[\mathbf{c}] = [\mathbf{A}\mathbf{w}] \in \mathcal{L}_\rho$ for $\rho = [\mathbf{A}] \in \mathbb{G}^{\ell \times k}$: Parse $pk_\rho = [\mathbf{p}^\top] \in \mathbb{G}^{1 \times k}$. $\Rightarrow [\pi] := [\mathbf{p}^\top] \cdot \mathbf{w} \in \mathbb{G}$.	$[\pi] \leftarrow \mathsf{Priv}(sk, [\mathbf{c}] \in \mathbb{G}^\ell)$: Parse $sk = \mathbf{k} \in \mathbb{Z}_p^\ell$. $\Rightarrow [\pi] := \mathbf{k}^\top \cdot [\mathbf{c}] \in \mathbb{G}$.

Fig. 7. Construction of LR-weak-ardent QAHPS over symmetric pairing groups.

The proof for Theorem 6 is just a simple adaptation of the proof for Theorem 2 over group $\mathbb{G}$.

The LR-weak-ardency of QAHPS follows from the theorem below. The proof of the theorem is just a simple adaptation of the proof for Theorem 3 over group $\mathbb{G}$.

Theorem 7 (LR-weak-ardency of QAHPS). *Let $\ell \geq 2k+1$ and $\kappa \leq \log p - \Omega(\lambda)$. The proposed* QAHPS *for $\mathscr{L}$ in Fig. 7 satisfies the properties listed in Table 2, i.e., (1) it is perfectly $\langle \bot, \bot \rangle$-universal and (2) it supports κ-LR-$\langle \mathscr{L}, \mathscr{L}_0 \rangle$-key-switching, where the language distributions $\mathscr{L} = \mathscr{L}_{\mathcal{D}_{\ell,k}}$ and $\mathscr{L}_0 = \mathscr{L}_{\mathcal{U}_{\ell,k}}$ are specified in Subsect. 6.2.*

6.4 The Instantiation of LR-Ardent QAHPS

We present the construction of $\widehat{\mathsf{QAHPS}} = (\widehat{\mathsf{Setup}}, \widehat{\alpha}_{(\cdot)}, \widehat{\mathsf{Pub}}, \widehat{\mathsf{Priv}})$ for $\mathscr{L}$ $(= \mathscr{L}_{\mathcal{D}_{\ell,k}})$ in Fig. 8. It is straightforward to check the perfect correctness of $\widehat{\mathsf{QAHPS}}$.

$\underline{\widehat{pp} \leftarrow_{\$} \widehat{\mathsf{Setup}}(1^\lambda)}$: $\mathcal{PG} = (\mathbb{G}, \mathbb{G}_T, p, e, P, P_T) \leftarrow_{\$} \mathsf{PGGen}(1^\lambda)$. $\Rightarrow \widehat{pp} := \mathcal{PG}$, which implicitly defines $(\widehat{\mathcal{SK}} := \mathbb{Z}_p^{\ell \times \ell},\ \widehat{\Pi} := \mathbb{G}_T,\ \widehat{\Lambda}_{(\cdot)})$, where $\widehat{\Lambda}_{\widehat{sk}}([\mathbf{c}]) := [\mathbf{c}]^\top \cdot \widehat{\mathbf{K}} \cdot [\mathbf{c}] \in \mathbb{G}_T$ for any $\widehat{sk} = \widehat{\mathbf{K}} \in \mathbb{Z}_p^{\ell \times \ell}$ and $[\mathbf{c}] \in \mathcal{X} = \mathbb{G}^\ell$.	$\widehat{pk}_\rho \leftarrow \widehat{\alpha}_\rho(\widehat{sk})$, where $\rho = [\mathbf{A}] \in \mathbb{G}^{\ell \times k}$: Parse $\widehat{sk} = \widehat{\mathbf{K}} \in \mathbb{Z}_p^{\ell \times \ell}$. $[\widehat{\mathbf{P}}]_T := [\mathbf{A}]^\top \cdot \widehat{\mathbf{K}} \cdot [\mathbf{A}] \in \mathbb{G}_T^{k \times k}$. $\Rightarrow \widehat{pk}_\rho := [\widehat{\mathbf{P}}]_T$.
$[\widehat{\pi}]_T \leftarrow \widehat{\mathsf{Pub}}(\widehat{pk}_\rho, [\mathbf{c}] \in \mathbb{G}^\ell, \mathbf{w} \in \mathbb{Z}_p^k)$, where $[\mathbf{c}] = [\mathbf{A}\mathbf{w}] \in \mathcal{L}_\rho$ for $\rho = [\mathbf{A}] \in \mathbb{G}^{\ell \times k}$: Parse $\widehat{pk}_\rho = [\widehat{\mathbf{P}}]_T \in \mathbb{G}_T^{k \times k}$. $\Rightarrow [\widehat{\pi}]_T := \mathbf{w}^\top \cdot [\widehat{\mathbf{P}}]_T \cdot \mathbf{w} \in \mathbb{G}_T$.	$[\widehat{\pi}]_T \leftarrow \widehat{\mathsf{Priv}}(\widehat{sk}, [\mathbf{c}] \in \mathbb{G}^\ell)$: Parse $\widehat{sk} = \widehat{\mathbf{K}} \in \mathbb{Z}_p^{\ell \times \ell}$. $\Rightarrow [\widehat{\pi}]_T := [\mathbf{c}]^\top \cdot \widehat{\mathbf{K}} \cdot [\mathbf{c}] \in \mathbb{G}_T$.

Fig. 8. Construction of LR-ardent $\widehat{\mathsf{QAHPS}}$ over symmetric pairing groups.

Theorem 8 (LR-ardency of $\widehat{\mathsf{QAHPS}}$). *Let $\ell \geq 2k+1$ and $\kappa \leq \log p - \Omega(\lambda)$. The proposed $\widehat{\mathsf{QAHPS}}$ scheme for $\mathscr{L}$ in Fig. 8 satisfies the properties listed in Table 2, i.e., (1) it is κ-LR-$\langle \mathscr{L}, \mathscr{L}_0 \rangle$- and* *perfectly $\langle \mathscr{L}_0, \mathscr{L}_1\rangle$-universal and (2) it supports κ-LR-$\langle \mathscr{L}, \mathscr{L}_0\rangle$-key-switching, where the language distributions $\mathscr{L} = \mathscr{L}_{\mathcal{D}_{\ell,k}}$, $\mathscr{L}_0 = \mathscr{L}_{\mathcal{U}_{\ell,k}}$ and $\mathscr{L}_1 = \mathscr{L}_{\mathcal{U}'_{\ell,k}}$ are specified in Subsect. 6.2.*

Proof of Theorem 8.

[Perfectly $\langle \mathscr{L}, \mathscr{L}_0\rangle$-Universal.] Let $(\rho = [\mathbf{A}] \in \mathbb{G}^{\ell\times k}, td) \leftarrow_\$ \mathscr{L}$ and $(\rho_0 = [\mathbf{A}_0] \in \mathbb{G}^{\ell\times k}, td_0) \leftarrow_\$ \mathscr{L}_0$. With overwhelming probability $1 - 2^{-\Omega(\lambda)}$, $(\mathbf{A}, \mathbf{A}_0) \in \mathbb{Z}_p^{\ell\times 2k}$ is of full column rank. For $\widehat{sk} = \widehat{\mathbf{K}} \leftarrow_\$ \mathbb{Z}_p^{\ell\times\ell}$ and any $[\mathbf{c}] \in \mathcal{X} \setminus (\mathcal{L}_\rho \cup \mathcal{L}_{\rho_0}) = \mathbb{G}^\ell \setminus (\mathsf{span}([\mathbf{A}]) \cup \mathsf{span}([\mathbf{A}_0]))$, we consider the distribution of $\widehat{\Lambda}_{\widehat{sk}}([\mathbf{c}])$ conditioned on $\widehat{pk}_\rho = \widehat{\alpha}_\rho(\widehat{sk})$ and $\widehat{pk}_{\rho_0} = \widehat{\alpha}_{\rho_0}(\widehat{sk})$.

Let $\mathbf{a}^\perp \in \mathbb{Z}_p^\ell$ (resp. $\mathbf{a}_0^\perp \in \mathbb{Z}_p^\ell$) be an arbitrary non-zero vector in the kernel space of $\mathbf{A}^\top$ (resp. $\mathbf{A}_0^\top$) such that $\mathbf{A}^\top \cdot \mathbf{a}^\perp = \mathbf{0}$ (resp. $\mathbf{A}_0^\top \cdot \mathbf{a}_0^\perp = \mathbf{0}$) holds. For the convenience of our analysis, we sample $\widehat{sk} = \widehat{\mathbf{K}} \leftarrow_\$ \mathbb{Z}_p^{\ell\times\ell}$ equivalently via

$$\widehat{sk} = \widehat{\mathbf{K}} := \widetilde{\mathbf{K}} + \mu \cdot \mathbf{a}_0^\perp \cdot (\mathbf{a}^\perp)^\top \in \mathbb{Z}_p^{\ell\times\ell},$$

where $\widetilde{\mathbf{K}} \leftarrow_\$ \mathbb{Z}_p^{\ell\times\ell}$ and $\mu \leftarrow_\$ \mathbb{Z}_p$. Consequently, we have

$$\widehat{pk}_\rho = \widehat{\alpha}_\rho(\widehat{sk}) = [\mathbf{A}]^\top \cdot \widehat{\mathbf{K}} \cdot [\mathbf{A}] = [\mathbf{A}]^\top \cdot \widetilde{\mathbf{K}} \cdot [\mathbf{A}],$$

$$\widehat{pk}_{\rho_0} = \widehat{\alpha}_{\rho_0}(\widehat{sk}) = [\mathbf{A}_0]^\top \cdot \widehat{\mathbf{K}} \cdot [\mathbf{A}_0] = [\mathbf{A}_0]^\top \cdot \widetilde{\mathbf{K}} \cdot [\mathbf{A}_0],$$

which may leak $\widetilde{\mathbf{K}}$, but the value of μ is completely hidden. Besides,

$$\widehat{\Lambda}_{\widehat{sk}}([\mathbf{c}]) = [\mathbf{c}]^\top \cdot \widehat{\mathbf{K}} \cdot [\mathbf{c}] = [\mathbf{c}]^\top \cdot \widetilde{\mathbf{K}} \cdot [\mathbf{c}] + \boxed{\mu \cdot [\mathbf{c}^\top \mathbf{a}_0^\perp] \cdot [\mathbf{c}^\top \mathbf{a}^\perp]^\top}.$$

Since $[\mathbf{c}] \notin \mathsf{span}([\mathbf{A}])$ and $[\mathbf{c}] \notin \mathsf{span}([\mathbf{A}_0])$, we can always find an $\mathbf{a}^\perp \in \mathbb{Z}_p^\ell$ such that $[\mathbf{c}^\top \mathbf{a}^\perp] \neq [0]$ holds and find an $\mathbf{a}_0^\perp \in \mathbb{Z}_p^\ell$ such that $[\mathbf{c}^\top \mathbf{a}_0^\perp] \neq [0]$ holds. Then, conditioned on $\widehat{pk}_\rho$ and $\widehat{pk}_{\rho_0}$, $\mu \cdot [\mathbf{c}^\top \mathbf{a}_0^\perp] \cdot [\mathbf{c}^\top \mathbf{a}^\perp]^\top$ is uniformly distributed over $\mathbb{G}_T$ due to the randomness of μ, so is $\widehat{\Lambda}_{\widehat{sk}}([\mathbf{c}])$.

This implies that $\widehat{\mathsf{QAHPS}}$ is perfectly $\langle \mathscr{L}, \mathscr{L}_0\rangle$-universal.

[Perfectly $\langle \mathscr{L}_0, \mathscr{L}_1\rangle$-Universal.] It can be proved in a similar way as the perfectly $\langle \mathscr{L}, \mathscr{L}_0\rangle$-universal.

[κ-LR-$\langle \mathscr{L}, \mathscr{L}_0\rangle$-Universal.] It follows from Lemma 7.

[κ-LR-$\langle \mathscr{L}, \mathscr{L}_0\rangle$-Key-Switching.] Let $(\rho = [\mathbf{A}] \in \mathbb{G}^{\ell\times k}, td) \leftarrow_\$ \mathscr{L}$ and let $L : \widehat{\mathcal{SK}} \longrightarrow \{0,1\}^\kappa$ be an arbitrary leakage function. For $\widehat{sk} = \widehat{\mathbf{K}} \leftarrow_\$ \mathbb{Z}_p^{\ell\times\ell}$, $\widehat{sk}' = \widehat{\mathbf{K}'} \leftarrow_\$ \mathbb{Z}_p^{\ell\times\ell}$ and $(\rho_0 = [\mathbf{A}_0] \in \mathbb{G}^{\ell\times k}, td_0) \leftarrow_\$ \mathscr{L}_0$, we aim to prove

$$\Delta\Big(\big(\underbrace{[\mathbf{A}_0]}_{\rho_0}, \underbrace{\boxed{[\mathbf{A}_0]^\top \widehat{\mathbf{K}} [\mathbf{A}_0]}}_{\widehat{\alpha}_{\rho_0}(\widehat{sk})} \big), \big(\underbrace{[\mathbf{A}_0]}_{\rho_0}, \underbrace{\boxed{[\mathbf{A}_0]^\top \widehat{\mathbf{K}'} [\mathbf{A}_0]}}_{\widehat{\alpha}_{\rho_0}(\widehat{sk}')} \big) \;\Big|\; \underbrace{[\mathbf{A}]^\top \widehat{\mathbf{K}} [\mathbf{A}]}_{\widehat{\alpha}_\rho(\widehat{sk})}, \; L(\widehat{\mathbf{K}}) \Big) \leq 2^{-\Omega(\lambda)}. \tag{19}$$

Similarly to the proof of (15) and by the multi-fold generalized leftover hash lemma (i.e., Lemma 4), we have that

$$\Delta\Big(\big([\mathbf{A}_0], \widehat{\mathbf{K}}[\mathbf{A}_0]\big), \big([\mathbf{A}_0], \widehat{\mathbf{K}'}[\mathbf{A}_0]\big) \;\Big|\; \widehat{\mathbf{K}}[\mathbf{A}], \; L(\widehat{\mathbf{K}}) \Big) \leq 2^{-\Omega(\lambda)}. \tag{20}$$

Note that (19) is deterministic in (20), then by Lemma 2, (19) holds.

This completes the proof of κ-LR-$\langle \mathscr{L}, \mathscr{L}_0\rangle$-key-switching. □

6.5 The Instantiation of LR-Weak-Ardent Tag-Based QAHPS

We present the construction of tag-based $\widetilde{\mathsf{QAHPS}} = (\widetilde{\mathsf{Setup}}, \widetilde{\alpha}_{(\cdot)}, \widetilde{\mathsf{Pub}}, \widetilde{\mathsf{Priv}})$ for the language distribution $\mathscr{L}$ $(= \mathscr{L}_{\mathcal{D}_{\ell,k}})$ in Fig. 9. It is straightforward to check the perfect correctness of $\widetilde{\mathsf{QAHPS}}$.

The LR-weak-ardency of $\widetilde{\mathsf{QAHPS}}$ follows from the theorem below. The proof of the theorem is just a simple adaptation of the proof for Theorem 5 over group $\mathbb{G}$.

Theorem 9 (LR-weak-ardency of Tag-Based $\widetilde{\mathsf{QAHPS}}$). *Let $\ell \geq 2k + 1$ and $\kappa \leq \log p - \Omega(\lambda)$. The proposed tag-based $\widetilde{\mathsf{QAHPS}}$ scheme for $\mathscr{L}$ in Fig. 9 satisfies the properties listed in Table 2, i.e., (1) it is $\langle \perp, \perp\rangle$-universal and (2) it supports κ-LR-$\langle \mathscr{L}, \mathscr{L}_0\rangle$- and $\langle \mathscr{L}_0, \mathscr{L}_1\rangle$-key-switching, where the language distributions $\mathscr{L} = \mathscr{L}_{\mathcal{D}_{\ell,k}}$, $\mathscr{L}_0 = \mathscr{L}_{\mathcal{U}_{\ell,k}}$ and $\mathscr{L}_1 = \mathscr{L}_{\mathcal{U}'_{\ell,k}}$ are specified in Subsect. 6.2.*

$\widetilde{pp} \leftarrow_{\$} \widetilde{\mathsf{Setup}}(1^\lambda)$: $\mathcal{PG} = (\mathbb{G}, \mathbb{G}_T, p, e, P, P_T) \leftarrow_{\$} \mathsf{PGGen}(1^\lambda)$. $\Rightarrow \widetilde{pp} := \mathcal{PG}$, which implicitly defines $(\widetilde{\mathcal{SK}} := \mathbb{Z}_p^{2\times\ell},\ \widetilde{\mathcal{T}} := \mathbb{G},\ \widetilde{\Pi} := \mathbb{G}_T,\ \widetilde{\Lambda}_{(\cdot)})$, where $\widetilde{\Lambda}_{\widetilde{sk}}([\mathbf{c}], [\tau]) := [1, \tau] \cdot \widetilde{\mathbf{K}} \cdot [\mathbf{c}] \in \mathbb{G}_T$ for any $\widetilde{sk} = \widetilde{\mathbf{K}} \in \mathbb{Z}_p^{2\times\ell}$, $[\mathbf{c}] \in \mathcal{X} = \mathbb{G}^\ell$ and $[\tau] \in \mathbb{G}$.	$\widetilde{pk}_\rho \leftarrow \widetilde{\alpha}_\rho(\widetilde{sk})$, where $\rho = [\mathbf{A}] \in \mathbb{G}^{\ell\times k}$: Parse $\widetilde{sk} = \widetilde{\mathbf{K}} \in \mathbb{Z}_p^{2\times\ell}$. $[\widetilde{\mathbf{P}}] := \widetilde{\mathbf{K}} \cdot [\mathbf{A}] \in \mathbb{G}^{2\times k}$. $\Rightarrow \widetilde{pk}_\rho := [\widetilde{\mathbf{P}}]$.
$[\widetilde{\pi}]_T \leftarrow \widetilde{\mathsf{Pub}}(\widetilde{pk}_\rho, [\mathbf{c}] \in \mathbb{G}^\ell, \mathbf{w} \in \mathbb{Z}_p^k, [\tau] \in \mathbb{G})$, where $[\mathbf{c}] = [\mathbf{A}\mathbf{w}] \in \mathcal{L}_\rho$ for $\rho = [\mathbf{A}] \in \mathbb{G}^{\ell\times k}$: Parse $\widetilde{pk}_\rho = [\widetilde{\mathbf{P}}] \in \mathbb{G}^{2\times k}$. $\Rightarrow [\widetilde{\pi}]_T := [1, \tau] \cdot [\widetilde{\mathbf{P}}] \cdot \mathbf{w} \in \mathbb{G}_T$.	$[\widetilde{\pi}]_T \leftarrow \widetilde{\mathsf{Priv}}(\widetilde{sk}, [\mathbf{c}] \in \mathbb{G}^\ell, [\tau] \in \mathbb{G})$: Parse $\widetilde{sk} = \widetilde{\mathbf{K}} \in \mathbb{Z}_p^{2\times\ell}$. $\Rightarrow [\widetilde{\pi}]_T := [1, \tau] \cdot \widetilde{\mathbf{K}} \cdot [\mathbf{c}] \in \mathbb{G}_T$.

Fig. 9. Construction of LR-weak-ardent tag-based $\widetilde{\mathsf{QAHPS}}$ over symmetric pairing groups.

6.6 Tightly LR-CCA-Secure PKE over Symmetric Pairing Groups

We are able to instantiate our generic construction of LR-CCA secure PKE in Sect. 4 with the LR-weak-ardent QAHPS (cf. Fig. 7), the LR-ardent $\widehat{\mathsf{QAHPS}}$ (cf. Fig. 8) and the LR-weak-ardent tag-based $\widetilde{\mathsf{QAHPS}}$ (cf. Fig. 9) over symmetric pairing groups $\mathcal{PG} = (\mathbb{G}, \mathbb{G}_T, p, e, P, P_T)$ based on the $\mathcal{D}_{\ell,k}$-MDDH assumptions. Observe that $\widehat{\Pi} = \widetilde{\Pi}$ in our instantiation, hence it supports the more efficient variant of generic PKE construction, as shown in Remark 8 and Fig. 15 in Appendix D. Let $\mathcal{H} = \{\mathsf{H} : \mathbb{G}^{\ell+1} \longrightarrow \mathbb{G}\}$ be a collision-resistant function family. We present the instantiation $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{sym}}$ with message space $\mathcal{M} = \mathbb{G}$ in Fig. 10. The scheme can be easily extended to encrypt vectors over $\mathbb{G}$, by replacing the vector $\mathbf{k}$ in the secret key with a matrix.

$\mathsf{PP} \leftarrow_{\$} \mathsf{Param}(1^\lambda)$: $\mathcal{PG} = (\mathbb{G}, \mathbb{G}_T, p, e, P, P_T) \leftarrow_{\$} \mathsf{PGGen}(1^\lambda)$. $\mathbf{A} \leftarrow_{\$} \mathcal{D}_{\ell,k}$. $\quad \mathsf{H} \leftarrow_{\$} \mathcal{H}$. $\Rightarrow \mathsf{PP} := (\mathcal{PG}, [\mathbf{A}], \mathsf{H})$.	$(\mathsf{PK}, \mathsf{SK}) \leftarrow_{\$} \mathsf{Gen}(\mathsf{PP})$: $\mathbf{k} \leftarrow_{\$} \mathbb{Z}_p^\ell$. $\quad [\mathbf{p}^\top] := \mathbf{k}^\top \cdot [\mathbf{A}] \in \mathbb{G}^{1\times k}$. $\widehat{\mathbf{K}} \leftarrow_{\$} \mathbb{Z}_p^{\ell\times\ell}$. $\quad [\widehat{\mathbf{P}}]_T := [\mathbf{A}]^\top \cdot \widehat{\mathbf{K}} \cdot [\mathbf{A}] \in \mathbb{G}_T^{k\times k}$. $\widetilde{\mathbf{K}} \leftarrow_{\$} \mathbb{Z}_p^{2\times\ell}$. $\quad [\widetilde{\mathbf{P}}] := \widetilde{\mathbf{K}} \cdot [\mathbf{A}] \in \mathbb{G}^{2\times k}$. $\Rightarrow \mathsf{PK} := ([\mathbf{p}], [\widehat{\mathbf{P}}]_T, [\widetilde{\mathbf{P}}])$, $\quad \mathsf{SK} := (\mathbf{k}, \widehat{\mathbf{K}}, \widetilde{\mathbf{K}})$.
$C \leftarrow_{\$} \mathsf{Enc}(\mathsf{PK}, [M] \in \mathbb{G})$: $\mathbf{w} \leftarrow_{\$} \mathbb{Z}_p^k$. $\quad [\mathbf{c}] := [\mathbf{A}]\mathbf{w} \in \mathbb{G}^\ell$. $[d] := [\mathbf{p}^\top] \cdot \mathbf{w} + [M] \in \mathbb{G}$. $[\tau] := \mathsf{H}([\mathbf{c}], [d]) \in \mathbb{G}$. $[\pi]_T := \underbrace{\mathbf{w}^\top \cdot [\widehat{\mathbf{P}}]_T \cdot \mathbf{w}}_{[\widehat{\pi}]_T} + \underbrace{[1, \tau] \cdot [\widetilde{\mathbf{P}}] \cdot \mathbf{w}}_{[\widetilde{\pi}]_T} \in \mathbb{G}_T$. $\Rightarrow C := ([\mathbf{c}], [d], [\pi]_T) \in \mathbb{G}^{\ell+1} \times \mathbb{G}_T$.	$[M]/\bot \leftarrow \mathsf{Dec}(\mathsf{SK}, C)$: Parse $C = ([\mathbf{c}], [d], [\pi']_T)$. $[M] := [d] - \mathbf{k}^\top \cdot [\mathbf{c}] \in \mathbb{G}$. $[\tau] := \mathsf{H}([\mathbf{c}], [d]) \in \mathbb{G}$. $[\pi]_T := \underbrace{[\mathbf{c}]^\top \cdot \widehat{\mathbf{K}} \cdot [\mathbf{c}]}_{[\widehat{\pi}]_T} + \underbrace{[1, \tau] \cdot \widetilde{\mathbf{K}} \cdot [\mathbf{c}]}_{[\widetilde{\pi}]_T} \in \mathbb{G}_T$. $\Rightarrow$ If $[\pi']_T = [\pi]_T$, Return $[M] \in \mathbb{G}$; Else, Return $\bot$.

Fig. 10. The instantiation $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{sym}}$ over symmetric pairing groups. The message space is $\mathcal{M} = \mathbb{G}$. Here $\mathcal{H} = \{\mathsf{H} : \mathbb{G}^{\ell+1} \longrightarrow \mathbb{G}\}$ is a collision-resistant function family.

For $\ell \geq 2k + 1$ and $\kappa \leq \log p - \Omega(\lambda)$, by combining Theorem 1 , Lemma 10 and Theorems 6, 7, 8, 9 together, we obtain the following corollary regarding the LR-CCA security of our instantiation $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{sym}}$.

Corollary 2 (LR-CCA Security of $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{sym}}$). *Let $\ell \geq 2k+1$ and $\kappa \leq \log p - \Omega(\lambda)$. If (i) the $\mathcal{D}_{\ell,k}$-MDDH assumption holds over $\mathbb{G}$, (ii) $\mathcal{H}$ is a collision-resistant function family, then the instantiation $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{sym}}$ in Fig. 10 is κ-LR-CCA secure. Concretely, for any adversary $\mathcal{A}$ who makes at most Q_e times of* Enc *queries and Q_d times of* Dec *queries, there exist adversaries $\mathcal{B}_1$ and $\mathcal{B}_2$, such that $\mathbf{T}(\mathcal{B}_2) \approx \mathbf{T}(\mathcal{A}) + (Q_e + Q_d) \cdot \mathsf{poly}(\lambda)$, $\mathbf{T}(\mathcal{B}_1) \approx \mathbf{T}(\mathcal{A}) + (Q_e + Q_e \cdot Q_d) \cdot \mathsf{poly}(\lambda)$, with $\mathsf{poly}(\lambda)$ independent of $\mathbf{T}(\mathcal{A})$, and*

$$\begin{aligned}\mathsf{Adv}^{\kappa\text{-}lr\text{-}cca}_{\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{sym}},\mathcal{A}}(\lambda) \leq{} & (4\lceil \log Q_e \rceil + \ell - k + 2) \cdot \mathsf{Adv}^{mddh}_{\mathcal{D}_{\ell,k},\mathbb{G},\mathcal{B}_1}(\lambda) + \mathsf{Adv}^{cr}_{\mathcal{H},\mathcal{B}_2}(\lambda) \\ & + (4 + Q_d + Q_d Q_e + \lceil \log Q_e \rceil \cdot (Q_d + Q_e + Q_d Q_e)) \cdot 2^{-\Omega(\lambda)}.\end{aligned}$$

Tight LR-CCA Security, Efficiency and Leakage-Rate of $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{sym}}$, and Extension to the Multi-User Setting. When $\mathcal{D}_{\ell,k} := \mathcal{U}_{\ell,k}$, the LR-CCA security of $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{sym}}$ is tightly reduced to the standard k-LIN assumption over symmetric pairing groups, since k-LIN implies $\mathcal{U}_{\ell,k}$-MDDH by Lemma 5. Let $k\mathbb{G}$ denote k elements in $\mathbb{G}$. By taking $\ell = 2k+1$, we have $\mathsf{PP} : (2k^2 + k)\mathbb{G}$, $\mathsf{PK} : 3k\mathbb{G} + k^2\mathbb{G}_T$, $\mathsf{SK} : (4k^2 + 10k + 4)\mathbb{Z}_p$, and $C : (2k+2)\mathbb{G} + 1\mathbb{G}_T$. See Table 1 for details. Furthermore, if we choose $\kappa = \log p - \Omega(\lambda)$, then the leakage-rate of the LR-CCA security is $\kappa/\mathsf{BitLength}(\mathsf{SK}) = \frac{1}{4k^2+10k+4} \cdot (1 - \frac{\Omega(\lambda)}{\log p})$, which is arbitrarily close to $1/(4k^2 + 10k + 4)$ if we choose a sufficiently large p.

Particularly, in case $k = 2$, the tight LR-CCA security of $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{sym}}$ is based on the 2-LIN assumption and it has $\mathsf{PK} : 6\mathbb{G} + 4\mathbb{G}_T$, $C : 6\mathbb{G} + 1\mathbb{G}_T$ and leakage-rate $= 1/40 - o(1)$.

The tight LR-CCA security of $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{sym}}$ also extends naturally to the multi-user setting, following the same analysis in Remark 10.

Remark 11. Our instantiations $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{asym}}$ in Fig. 6 and $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{sym}}$ in Fig. 10 can be changed into non-LR but more efficient PKE schemes, namely $\mathsf{PKE}_{\mathsf{asym}}$ and $\mathsf{PKE}_{\mathsf{sym}}$, by setting $\ell = 2k$ (instead of $\ell \geq 2k+1$). Without key leakage, primitives $\mathsf{QAHPS}, \widehat{\mathsf{QAHPS}}$ and tag-based $\widetilde{\mathsf{QAHPS}}$ parameterized with $\ell = 2k$ can be proved to be *perfectly* universal and *perfectly* key-switching, which implies 0-LR-(weak-)ardency. Consequently, $\mathsf{PKE}_{\mathsf{asym}}$ and $\mathsf{PKE}_{\mathsf{sym}}$ have tight multi-challenge (and multi-user) IND-CCA security.

Acknowledgments. We would like to thank the anonymous reviewers for their comments and suggestions. We are grateful to Dennis Hofheinz and Jiaxin Pan for helpful discussions and advices. Shuai Han, Shengli Liu and Lin Lyu are supported by the National Natural Science Foundation of China Grant (No. 61672346). Dawu Gu is supported by the National Natural Science Foundation of China Grant (No. U1636217) together with Program of Shanghai Academic Research Leader (16XD1401300).

References

[ABP15] Abdalla, M., Benhamouda, F., Pointcheval, D.: Disjunctions for hash proof systems: New constructions and applications. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015, Part II, LNCS, vol. 9057, pp. 69–100. Springer (2015)

[ADK+13] Abe, M., David, B., Kohlweiss, M., Nishimaki, R., Ohkubo, M.: Tagged one-time signatures: Tight security and optimal tag size. In: Kurosawa, K., Hanaoka, G. (eds.) PKC 2013, LNCS, vol. 7778, pp. 312–331. Springer (2013)

[ADN+10] Alwen, J., Dodis, Y., Naor, M., Segev, G., Walfish, S., Wichs, D.: Public-key encryption in the bounded-retrieval model. In: Gilbert, H. (ed.) EUROCRYPT 2010, LNCS, vol. 6110, pp. 113–134. Springer (2010)

[AGV09] Akavia, A., Goldwasser, S., Vaikuntanathan, V.: Simultaneous hardcore bits and cryptography against memory attacks. In: Reingold, O. (ed.) TCC 2009, LNCS, vol. 5444, pp. 474–495 (2009)

[AHY15] Attrapadung, N., Hanaoka, G., Yamada, S.: A framework for identity-based encryption with almost tight security. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015, Part I, LNCS, vol. 9452, pp. 521–549. Springer (2015)

[AJOR18a] Abe, M., Jutla, C.S., Ohkubo, M., Roy, A.: Improved (almost) tightly-secure simulation-sound QA-NIZK with applications. In: Peyrin, T., Galbraith, S.D. (eds.) ASIACRYPT 2018, Part I, LNCS, vol. 11272, pp. 627–656. Springer (2018)

[AJOR18b] Abe, M., Jutla, C.S., Ohkubo, M., Roy, A.: Improved (almost) tightly-secure simulation-sound QA-NIZK with applications. IACR Cryptology ePrint Archive, Report 2018/849 (2018), http://eprint.iacr.org/2018/849/20190207:025738

[BBM00] Bellare, M., Boldyreva, A., Micali, S.: Public-key encryption in a multi-user setting: Security proofs and improvements. In: Preneel, B. (ed.) EUROCRYPT 2000, LNCS, vol. 1807, pp. 259–274 (2000)

[CS02] 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 (2002)

[CS04] Cramer, R., Shoup, V.: Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM J. Comput. vol. 33(1), pp. 167–226 (2004)

[CW13] Chen, J., Wee, H.: Fully, (almost) tightly secure IBE and dual system groups. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part II, pp. 435–460 (2013)

[DHLAW10] Dodis, Y., Haralambiev, K., López-Alt, A., Wichs, D.: Efficient public-key cryptography in the presence of key leakage. In: Abe, M. (ed.) ASIACRYPT 2010, LNCS, vol. 6477, pp. 613–631 (2010)

[DKPW12] Dodis, Y., Kiltz, E., Pietrzak, K., Wichs, D.: Message authentication, revisited. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012, pp. 355–374 (2012)

[DORS08] Dodis, Y., Ostrovsky, R., Reyzin, L., Smith, A.: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. SIAM J. Comput. vol. 38(1), pp. 97–139 (2008)

[EHK+13] Escala, A., Herold, G., Kiltz, E., Ràfols, C., Villar, J.L.: An algebraic framework for Diffie-Hellman assumptions. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part II, pp. 129–147 (2013)

[FV16] Faonio, A., Venturi, D.: Efficient public-key cryptography with bounded leakage and tamper resilience. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part I, LNCS, vol. 10031, pp. 877–907 (2016)

[FX16] Fujisaki, E., Xagawa, K.: Public-key cryptosystems resilient to continuous tampering and leakage of arbitrary functions. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part I, LNCS, vol. 10031, pp. 908–938 (2016)

[GCD+16] Gong, J., Chen, J., Dong, X., Cao, Z., Tang, S.: Extended nested dual system groups, revisited. In: Cheng, C., Chung, K., Persiano, G., Yang, B. (eds.) PKC 2016, Part I, pp. 133–163 (2016)

[GHK17] Gay, R., Hofheinz, D., Kohl, L.: Kurosawa-Desmedt meets tight security. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017, Part III, LNCS, vol. 10403, pp. 133–160. Springer (2017)

[GHKP18] Gay, R., Hofheinz, D., Kohl, L., Pan, J.: More efficient (almost) tightly secure structure-preserving signatures. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018, Part II, LNCS, vol. 10821, pp. 230–258. Springer (2018)

[GHKW16] Gay, R., Hofheinz, D., Kiltz, E., Wee, H.: Tightly CCA-secure encryption without pairings. In: Fischlin, M., Coron, J. (eds.) EUROCRYPT 2016, Part I, pp. 1–27 (2016)

[HJ12] Hofheinz, D., Jager, T.: Tightly secure signatures and public-key encryption. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012, LNCS, vol. 7417, pp. 590–607 (2012)

[Hof16] Hofheinz, D.: Algebraic partitioning: Fully compact and (almost) tightly secure cryptography. In: Kushilevitz, E., Malkin, T. (eds.) TCC 2016-A, Part I, LNCS, vol. 9562, pp. 251–281. Springer (2016)

[Hof17] Hofheinz, D.: Adaptive partitioning. In: Coron, J., Nielsen, J.B. (eds.) EUROCRYPT 2017, Part III, LNCS, vol. 10212, pp. 489–518 (2017)

[HSH+08] Halderman, J.A., Schoen, S.D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J.A., Feldman, A.J., Appelbaum, J., Felten, E.W.: Lest we remember: Cold boot attacks on encryption keys. In: van Oorschot, P.C. (ed.) USENIX Security Symposium 2008, pp. 45–60. USENIX Association (2008)

[JR13] Jutla, C.S., Roy, A.: Shorter quasi-adaptive NIZK proofs for linear subspaces. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part I, LNCS, vol. 8269, pp. 1–20 (2013)

[JR15] Jutla, C.S., Roy, A.: Dual-system simulation-soundness with applications to UC-PAKE and more. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015, Part I, LNCS, vol. 9452, pp. 630–655. Springer (2015)

[KD04] Kurosawa, K., Desmedt, Y.: A new paradigm of hybrid encryption scheme. In: Franklin, M.K. (ed.) CRYPTO 2004, LNCS, vol. 3152, pp. 426–442. Springer (2004)

[KW15] Kiltz, E., Wee, H.: Quasi-adaptive NIZK for linear subspaces revisited. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015, Part II, LNCS, vol. 9057, pp. 101–128. Springer (2015)

[LPJY14] Libert, B., Peters, T., Joye, M., Yung, M.: Non-malleability from malleability: Simulation-sound quasi-adaptive NIZK proofs and CCA2-secure encryption from homomorphic signatures. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014, LNCS, vol. 8441, pp. 514–532. Springer (2014)

[LPJY15] Libert, B., Peters, T., Joye, M., Yung, M.: Compactly hiding linear spans - tightly secure constant-size simulation-sound QA-NIZK proofs and applications. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015, Part I, pp. 681–707 (2015)

[NS09] Naor, M., Segev, G.: Public-key cryptosystems resilient to key leakage. In: Halevi, S. (ed.) CRYPTO 2009, pp. 18–35 (2009)

[NY90] Naor, M., Yung, M.: Public-key cryptosystems provably secure against chosen ciphertext attacks. In: Ortiz, H. (ed.) STOC 1990, pp. 427–437. ACM (1990)

[QL13] Qin, B., Liu, S.: Leakage-resilient chosen-ciphertext secure public-key encryption from hash proof system and one-time lossy filter. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part II, LNCS, vol. 8270, pp. 381–400. Springer (2013)

[QLC15] Qin, B., Liu, S., Chen, K.: Efficient chosen-ciphertext secure public-key encryption scheme with high leakage-resilience. IET Information Security vol. 9(1), pp. 32–42 (2015)

[Sho06] Shoup, V.: A computational introduction to number theory and algebra. Cambridge University Press (2006)

[WC81] Wegman, M.N., Carter, L.: New hash functions and their use in authentication and set equality. Journal of Computer and System Sciences vol. 22(3), pp. 265–279 (1981)

[Wee12] Wee, H.: Dual projective hashing and its applications - lossy trapdoor functions and more. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012, pp. 246–262 (2012)

A Formal Definitions

A.1 LR-CCA Security in the Multi-User Setting

Definition 13 (Multi-Ciphertext κ-LR-CCA Security in the Multi-User Setting). *Let $\kappa = \kappa(\lambda)$. A PKE scheme* PKE *is κ-LR-CCA secure in the multi-user setting, if for any PPT adversary $\mathcal{A}$, any polynomial $Q_u = \mathsf{poly}(\lambda)$, it holds that*

$$\mathsf{Adv}^{(\kappa,Q_u)\text{-}lr\text{-}cca}_{\mathsf{PKE},\mathcal{A}}(\lambda) := \left|\Pr[(\kappa,Q_u)\text{-}\mathsf{lr}\text{-}\mathsf{cca}^{\mathcal{A}} \Rightarrow 1] - \tfrac{1}{2}\right| \leq \mathsf{negl}(\lambda),$$

where game (κ, Q_u)-lr-cca in the multi-user setting is specified in Fig. 11.

If $Q_u = 1$, the security is reduced to the (single-user) LR-CCA security as defined in Definition 2.

Proc. INITIALIZE:	**Proc.** LEAK(L, j):	**Proc.** ENC(M_0, M_1, j):	**Proc.** DEC(C, j):
$\mathsf{PP} \leftarrow_\$ \mathsf{Param}(1^\lambda)$. $\beta \leftarrow_\$ \{0,1\}$. // challenge bit For $j \in [Q_u]$, $(\mathsf{PK}_j, \mathsf{SK}_j) \leftarrow_\$ \mathsf{Gen}(\mathsf{PP})$. $l_j := 0$. // bit length of leakage $\mathsf{chal} := \mathsf{false}$. Return $(\mathsf{PP}, (\mathsf{PK}_j)_{j\in[Q_u]})$.	If $(\mathsf{chal} = \mathsf{true})$ $\vee\ (l_j + \lvert L(\mathsf{SK}_j)\rvert > \kappa)$, Return $\perp$. $l_j := l_j + \lvert L(\mathsf{SK}_j)\rvert$. Return $L(\mathsf{SK}_j)$.	$\mathsf{chal} := \mathsf{true}$. If $\lvert M_0\rvert \neq \lvert M_1\rvert$, Return $\perp$. $C^* \leftarrow_\$ \mathsf{Enc}(\mathsf{PK}_j, M_\beta)$. $\mathcal{Q}_{\mathcal{ENC},j} := \mathcal{Q}_{\mathcal{ENC},j} \cup \{C^*\}$. Return C^*.	If $C \in \mathcal{Q}_{\mathcal{ENC},j}$, Return $\perp$. Return $\mathsf{Dec}(\mathsf{SK}_j, C)$. **Proc.** FINALIZE$(\beta')$: Return $(\beta' = \beta)$.

Fig. 11. (κ, Q_u)-lr-cca security game for PKE in the multi-user setting.

A.2 Hash Proof System

Hash proof system (HPS) was proposed by Cramer and Shoup in the seminal work [CS02], and turned out to be a very powerful tool in a wide range of applications, such as PKE and KEM [CS04, KD04]. We give the formal definition according to [CS02].

Definition 14 (Hash Proof System). *A hash proof system* $\mathsf{HPS} = (\mathsf{Setup}, \mathsf{Pub}, \mathsf{Priv})$ *consists of a tuple of PPT algorithms:*

- $pp \leftarrow_\$ \mathsf{Setup}(1^\lambda)$*: The setup algorithm outputs a public parameter pp, which implicitly defines $(\mathcal{L}, \mathcal{X}, \mathcal{SK}, \mathcal{PK}, \Pi, \Lambda_{(\cdot)}, \alpha)$, where $\mathcal{L} \subseteq \mathcal{X}$ is an NP-language with universe $\mathcal{X}$, $\mathcal{SK}$ is the hashing key space, $\mathcal{PK}$ is the projection key space, Π is the hash value space, $\Lambda_{(\cdot)} : \mathcal{X} \longrightarrow \Pi$ is a family of hash functions indexed by a hashing key $sk \in \mathcal{SK}$, and $\alpha : \mathcal{SK} \longrightarrow \mathcal{PK}$ is the projection function.*
  We assume that $\Lambda_{(\cdot)}$ and α are efficiently computable and there are PPT algorithms for sampling $x \leftarrow_\$ \mathcal{L}$ uniformly together with a witness w, sampling $x \leftarrow_\$ \mathcal{X}$ uniformly, and sampling $sk \leftarrow_\$ \mathcal{SK}$ uniformly. We require pp to be an implicit input of other algorithms.
- $\pi \leftarrow \mathsf{Pub}(pk, x, w)$*: The public evaluation algorithm outputs the hash value $\pi = \Lambda_{sk}(x) \in \Pi$ of $x \in \mathcal{L}$, with the help of a projection key $pk = \alpha(sk)$ and a witness w for $x \in \mathcal{L}$.*
- $\pi \leftarrow \mathsf{Priv}(sk, x)$*: The private evaluation algorithm outputs the hash value $\pi = \Lambda_{sk}(x) \in \Pi$ of $x \in \mathcal{X}$, directly using the hashing key sk.*

Perfect correctness *(a.k.a. projectiveness) of* HPS *requires that, for all possible $pp \leftarrow_\$ \mathsf{Setup}(1^\lambda)$, all hashing keys $sk \in \mathcal{SK}$ with $pk := \alpha(sk)$ the corresponding projection key, all $x \in \mathcal{L}$ with all possible witnesses w, it holds that*

$$\mathsf{Pub}(pk, x, w) \ = \ \Lambda_{sk}(x) \ = \ \mathsf{Priv}(sk, x).$$

B The Non-Triviality for Achieving Tight LR-CCA

In this work, we employed ardent QAHPS as an important building block, and illustrated in detail that the "universal" and "key-switching" properties of QAHPS do hold in the LR setting. Moreover, we designed our LR-CCA secure PKE by combining several LR-ardent QAHPS schemes carefully and we instantiated these QAHPS from the MDDH assumptions.

For example, for the PKE instantiation over asymmetric pairing groups (i.e., the $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{asym}}$ in Fig. 6), the instance $x^* = ([\mathbf{A}_1\mathbf{w}_1]_1, [\mathbf{A}_2\mathbf{w}_2]_2) \leftarrow_{\$} \mathcal{L}_\rho (= \mathsf{span}([\mathbf{A}_1]_1) \times \mathsf{span}([\mathbf{A}_2]_2))$ in challenge ciphertext can be changed to $x^* = ([\mathbf{A}_{0,1}\mathbf{w}_1]_1, [\mathbf{A}_{0,2}\mathbf{w}_2]_2) \leftarrow_{\$} \mathcal{L}_{\rho_0} (= \mathsf{span}([\mathbf{A}_{0,1}]_1) \times \mathsf{span}([\mathbf{A}_{0,2}]_2))$ in the LR-CCA security proof, due to the MDDH assumption. An important observation is that the adversary does not know $\rho_0 = ([\mathbf{A}_{0,1}]_1, [\mathbf{A}_{0,2}]_2)$ before the challenge ciphertexts are generated. Meanwhile, $\mathcal{A}$ is not allowed to query key leakage after it sees the first challenge ciphertext. Consequently, the leakage function $L(\cdot)$ submitted by $\mathcal{A}$ is definitely independent of $([\mathbf{A}_{0,1}]_1, [\mathbf{A}_{0,2}]_2)$, so $([\mathbf{A}_{0,1}]_1, [\mathbf{A}_{0,2}]_2)$ can behave as an index of a universal hash function and applies to the secret key of QAHPS. As a result, the (multi-fold) generalized leftover hash lemma guarantees that the LR-universal and the LR-key-switching hold for QAHPS, which make possible the LR-CCA security proof of our $\mathsf{PKE}^{\mathsf{lr}}_{\mathsf{asym}}$.

In contrast, Gay et al. [GHK17] used "qualified proof system" (QPS) in their PKE construction, and the tight IND-CCA security of PKE depends on the "constrained soundness" and "extensibility" properties of QPS. However, the proofs for these two properties seem hard to be adapted to the LR setting. The technical reasons are as follows.

1) "Constrained soundness" of [GHK17]'s QPS might not hold in the LR setting.
Note that [GHK17] employed two universal hash functions h_0 and h_1 in their QPS construction, which help to map the group elements in $\mathbb{G}$ back to the scalars in $\mathbb{Z}_p$. In the "constrained soundness" proof (cf. [GHK17, Lemma 6]), they applied the Leftover Hash Lemma (LHL) to argue that the outputs of h_0 and h_1 are uniformly distributed. For example, in the last game of the proof, $\mathbf{y} = \mathsf{h}_1(\mathbf{K}_\mathbf{y}[\mathbf{c}])$ is uniform due to LHL. However, this argument is invalid in the LR setting, due to the inapplicability of LHL. This is because, the (generalized) LHL (cf. Lemma 3) works only if the auxiliary information about the input is independent of the universal hash function h_1, while here the leakage information $L(\mathbf{K}_\mathbf{X}, \mathbf{K}_\mathbf{y})$ might depend on h_1, since the leakage function L is chosen by the adversary after obtaining h_1 from the public parameters.

2) "Extensibility" of [GHK17]'s QPS might not hold in the LR setting.
In the "extensibility" proof (cf. [GHK17, Lemma 7]), they essentially argued that $(\mathbf{K}_\mathbf{X}\mathbf{A}, \mathbf{K}_\mathbf{X}\mathbf{A}_0)$ is identically distributed to $(\mathbf{K}_\mathbf{X}\mathbf{A}, \widetilde{\mathbf{K}}_\mathbf{X}\mathbf{A}_0)$, thus the proof system PS is indistinguishable from $\widetilde{\mathsf{PS}}$. However, this argument is invalid in the LR setting. For example, the adversary may simply let $L(\mathbf{K}_\mathbf{X}, \mathbf{K}_\mathbf{y})$ be the first few bits of $\mathbf{K}_\mathbf{X}\mathbf{A}_0$ (note that $\mathbf{A}_0$ is contained in the public parameters), thus can trivially distinguish $(\mathbf{K}_\mathbf{X}\mathbf{A}, \mathbf{K}_\mathbf{X}\mathbf{A}_0)$ from $(\mathbf{K}_\mathbf{X}\mathbf{A}, \widetilde{\mathbf{K}}_\mathbf{X}\mathbf{A}_0)$. (We stress that, in contrast, the "key-switching" property of our QAHPS works well in the LR setting smoothly, since $\mathbf{A}_0$ is not contained in our public parameters and is not leaked to the adversary unless the adversary finished the leakage queries.)

Besides the above observations, there are also some other game hops in [GHK17] that seem hard to be adapted to the LR setting. As such, it is reasonable to conjecture that the tightly IND-CCA secure PKE proposed in [GHK17] is not leakage-resilient.

C Game-Based Definition for Leakage-Resilient Ardency of QAHPS

We present game-based definition for LR-ardency of QAHPS by defining κ-LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-universal and κ-LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-key-switching properties via games.

Definition 15 (Leakage-Resilient Ardent QAHPS, Game-Based Version). *Let $\kappa = \kappa(\lambda) \in \mathbb{N}$, and let $\mathscr{L}_0, \mathscr{L}_1$ be a pair of language distributions. A QAHPS scheme $\mathsf{QAHPS} = (\mathsf{Setup}, \alpha_{(\cdot)}, \mathsf{Pub}, \mathsf{Priv})$ for a language distribution $\mathscr{L}$ is called κ-leakage-resilient $\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-ardent ($\kappa$-LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-ardent), if the following two properties hold:*

- **(κ-LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-Universal).** *For any (possibly unbounded) adversary $\mathcal{A}$, it holds that*

$$\Pr[\kappa\text{-}\mathsf{lr}\text{-}\mathsf{universal}^{\mathcal{A}} \Rightarrow 1] \leq 2^{-\Omega(\lambda)},$$

  where game κ-lr-$\mathsf{universal}$ is specified in Fig. 12.

<u>**Proc.** INITIALIZE:</u>	<u>**Proc.** LEAK(L):</u>	<u>**Proc.** FINALIZE(x, π):</u>
$pp \leftarrow_\$ \mathsf{Setup}(1^\lambda)$. $(\rho_0, td_0) \leftarrow_\$ \mathscr{L}_0$. $(\rho_1, td_1) \leftarrow_\$ \mathscr{L}_1$. $sk \leftarrow_\$ \mathcal{SK}$. $l := 0$. // bit length of leakage Return $(pp, \rho_0, \rho_1, \alpha_{\rho_0}(sk), \alpha_{\rho_1}(sk))$.	If $(l + \lvert L(sk) \rvert > \kappa)$, Return $\perp$. $l := l + \lvert L(sk) \rvert$. Return $L(sk)$.	If $(x \in \mathcal{X} \setminus (\mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1}))$ $\wedge\ (\pi = \Lambda_{sk}(x))$, Return 1. Return 0.

Fig. 12. κ-lr-$\mathsf{universal}$ security game for QAHPS.

- **(κ-LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-Key-Switching).** *For any (possibly unbounded) adversary $\mathcal{A}$, it holds that*

$$\left| \Pr[\kappa\text{-}\mathsf{lr}\text{-}\mathsf{key}\text{-}\mathsf{switching}^{\mathcal{A}} \Rightarrow 1] - \tfrac{1}{2} \right| \leq 2^{-\Omega(\lambda)},$$

  where game κ-lr-key-$\mathsf{switching}$ is specified in Fig. 13.

<u>**Proc.** INITIALIZE:</u>	<u>**Proc.** LEAK(L):</u>	<u>**Proc.** CHAL():</u>
$pp \leftarrow_\$ \mathsf{Setup}(1^\lambda)$. $(\rho_0, td_0) \leftarrow_\$ \mathscr{L}_0$. $(\rho_1, td_1) \leftarrow_\$ \mathscr{L}_1$. $sk, sk' \leftarrow_\$ \mathcal{SK}$. $\beta \leftarrow_\$ \{0,1\}$. // challenge bit $l := 0$. // bit length of leakage $\mathsf{chal} := \mathsf{false}$. Return $(pp, \rho_0, \alpha_{\rho_0}(sk))$.	If $(\mathsf{chal} = \mathsf{true})$ $\vee\ (l + \lvert L(sk) \rvert > \kappa)$, Return $\perp$. $l := l + \lvert L(sk) \rvert$. Return $L(sk)$.	$\mathsf{chal} := \mathsf{true}$. If $\beta = 0$, Return $(\rho_1, \alpha_{\rho_1}(sk))$. Else $\beta = 1$, Return $(\rho_1, \alpha_{\rho_1}(sk'))$. <u>**Proc.** FINALIZE($\beta'$):</u> Return $(\beta' = \beta)$.

Fig. 13. κ-lr-key-$\mathsf{switching}$ security game for QAHPS.

Similarly, game-based definition for LR-ardency of tag-based QAHPS is presented as follows.

Definition 16 (Leakage-Resilient Ardent Tag-Based QAHPS, Game-Based Version). *Let $\kappa = \kappa(\lambda) \in \mathbb{N}$, and let $\mathscr{L}_0, \mathscr{L}_1$ be a pair of language distributions. A tag-based QAHPS scheme $\mathsf{QAHPS} = (\mathsf{Setup}, \alpha_{(\cdot)}, \mathsf{Pub}, \mathsf{Priv})$ for a language distribution $\mathscr{L}$ is called κ-leakage-resilient $\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-ardent ($\kappa$-LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-ardent), if the following two properties hold:*

- **(κ-LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-Universal for Tag-Based QAHPS).** *For any (possibly unbounded) adversary $\mathcal{A}$, it holds that*

$$\Pr[\kappa\text{-}\mathsf{lr}\text{-}\mathsf{tag}\text{-}\mathsf{universal}^{\mathcal{A}} \Rightarrow 1] \leq 2^{-\Omega(\lambda)},$$

  where game κ-lr-tag-$\mathsf{universal}$ is specified in Fig. 14.

- **(κ-LR-$\langle \mathscr{L}_0, \mathscr{L}_1 \rangle$-Key-Switching for Tag-Based QAHPS).** *This property is the same as that defined for the non-tag-based QAHPS in Definition 15, since no tag is involved in the projection algorithm $\alpha_{(\cdot)}$.*

Proc. Initialize: $pp \leftarrow_\$ \mathsf{Setup}(1^\lambda)$. $(\rho_0, td_0) \leftarrow_\$ \mathscr{L}_0$. $(\rho_1, td_1) \leftarrow_\$ \mathscr{L}_1$. $sk \leftarrow_\$ \mathcal{SK}$. $l := 0$. // bit length of leakage $\mathsf{chal} := \mathsf{false}$. Return $(pp,\ \rho_0,\ \rho_1,\ \alpha_{\rho_0}(sk),\ \alpha_{\rho_1}(sk))$.	**Proc.** Leak(L): If $(\mathsf{chal} = \mathsf{true})$ $\vee\ (l + \lvert L(sk)\rvert > \kappa)$, Return $\perp$. $l := l + \lvert L(sk)\rvert$. Return $L(sk)$.	**Proc.** Chal(x', τ'): $\mathsf{chal} := \mathsf{true}$. Return $\Lambda_{sk}(x', \tau')$. **Proc.** Finalize(x, τ, π): If $(x \in \mathcal{X} \setminus (\mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1}))$ $\wedge\ (\tau \neq \tau') \wedge (\pi = \Lambda_{sk}(x, \tau))$, Return 1. Return 0.

Fig. 14. κ-lr-tag-universal security game for tag-based QAHPS.

D A More Efficient Variant of Generic PKE Construction

See Fig. 15.

$\mathsf{PP} \leftarrow_\$ \mathsf{Param}(1^\lambda)$: $pp \leftarrow_\$ \mathsf{Setup}(1^\lambda)$, which defines $(\mathcal{SK}, \Pi, \Lambda_{(\cdot)})$. $\widehat{pp} \leftarrow_\$ \widehat{\mathsf{Setup}}(1^\lambda)$, which defines $(\widehat{\mathcal{SK}}, \widehat{\Pi}, \widehat{\Lambda}_{(\cdot)})$. $\widetilde{pp} \leftarrow_\$ \widetilde{\mathsf{Setup}}(1^\lambda)$, which defines $(\widetilde{\mathcal{SK}}, \widetilde{\mathcal{T}}, \widetilde{\Pi}, \widetilde{\Lambda}_{(\cdot)})$. $(\rho, td) \leftarrow_\$ \mathscr{L}$. $\mathsf{H} \leftarrow_\$ \mathcal{H}$. $\Rightarrow \mathsf{PP} := (pp, \widehat{pp}, \widetilde{pp}, \rho, \mathsf{H})$.	$(\mathsf{PK}, \mathsf{SK}) \leftarrow_\$ \mathsf{Gen}(\mathsf{PP})$: $sk \leftarrow_\$ \mathcal{SK}$. $pk_\rho := \alpha_\rho(sk)$. $\widehat{sk} \leftarrow_\$ \widehat{\mathcal{SK}}$. $\widehat{pk}_\rho := \widehat{\alpha}_\rho(\widehat{sk})$. $\widetilde{sk} \leftarrow_\$ \widetilde{\mathcal{SK}}$. $\widetilde{pk}_\rho := \widetilde{\alpha}_\rho(\widetilde{sk})$. $\Rightarrow \mathsf{PK} := (pk_\rho, \widehat{pk}_\rho, \widetilde{pk}_\rho)$, $\mathsf{SK} := (sk, \widehat{sk}, \widetilde{sk})$.
$C \leftarrow_\$ \mathsf{Enc}(\mathsf{PK}, M)$: $x \leftarrow_\$ \mathcal{L}_\rho$ with witness w. $d := \mathsf{Pub}(pk_\rho, x, w) + M \in \Pi$. $\tau := \mathsf{H}(x, d) \in \widetilde{\mathcal{T}}$. $\pi := \underbrace{\widehat{\mathsf{Pub}}(\widehat{pk}_\rho, x, w)}_{\widehat{\pi}} + \underbrace{\widetilde{\mathsf{Pub}}(\widetilde{pk}_\rho, x, w, \tau)}_{\widetilde{\pi}} \in \widehat{\Pi}$. $\Rightarrow C := (x, d, \pi)$.	$M / \perp \leftarrow \mathsf{Dec}(\mathsf{SK}, C)$: Parse $C = (x, d, \pi')$. $M := d - \mathsf{Priv}(sk, x) \in \Pi$. $\tau := \mathsf{H}(x, d) \in \widetilde{\mathcal{T}}$. $\pi := \underbrace{\widehat{\mathsf{Priv}}(\widehat{sk}, x)}_{\widehat{\pi}} + \underbrace{\widetilde{\mathsf{Priv}}(\widetilde{sk}, x, \tau)}_{\widetilde{\pi}} \in \widehat{\Pi}$. $\Rightarrow$ If $\pi' = \pi$, Return M; Else, Return $\perp$.

Fig. 15. A more efficient construction of PKE from QAHPS, $\widehat{\mathsf{QAHPS}}$ and tag-based $\widetilde{\mathsf{QAHPS}}$ when $\widehat{\Pi} = \widetilde{\Pi}$.

E Figures for Proof of Theorem 1

$\mathsf{G}_0 - \mathsf{G}_6$, $\mathsf{G}_1 - \mathsf{G}_6$, $\mathsf{G}_2 - \mathsf{G}_6$, $\mathsf{G}_3 - \mathsf{G}_6$, $\mathsf{G}_4 - \mathsf{G}_6$, $\mathsf{G}_5 - \mathsf{G}_6$, G_6

<u>INITIALIZE:</u>

$pp \leftarrow_\$ \mathsf{Setup}(1^\lambda)$.
$\widehat{pp} \leftarrow_\$ \widehat{\mathsf{Setup}}(1^\lambda)$.
$\widetilde{pp} \leftarrow_\$ \widetilde{\mathsf{Setup}}(1^\lambda)$.
$(\rho, td) \leftarrow_\$ \mathscr{L}$.
$(\rho_0, td_0) \leftarrow_\$ \mathscr{L}_0$.
$\mathsf{H} \leftarrow_\$ \mathcal{H}$.
$\mathsf{PP} := (pp, \widehat{pp}, \widetilde{pp}, \rho, \mathsf{H})$.
sk, sk' $\leftarrow_\$ \mathcal{SK}$.
$\widehat{sk} \leftarrow_\$ \widehat{\mathcal{SK}}$.
$\widetilde{sk} \leftarrow_\$ \widetilde{\mathcal{SK}}$.
$pk_\rho := \alpha_\rho(sk)$.
$\widehat{pk}_\rho := \widehat{\alpha}_\rho(\widehat{sk})$.
$\widetilde{pk}_\rho := \widetilde{\alpha}_\rho(\widetilde{sk})$.
$\mathsf{PK} := (pk_\rho, \widehat{pk}_\rho, \widetilde{pk}_\rho)$.
$\mathsf{SK} := (sk, \widehat{sk}, \widetilde{sk})$.
$\beta \leftarrow_\$ \{0,1\}$.
// challenge bit
$l := 0$.
// bit length of leakage
$\mathsf{chal} := \mathsf{false}$.
$\Rightarrow (\mathsf{PP}, \mathsf{PK})$.

<u>LEAK(L):</u>

If ($\mathsf{chal} = \mathsf{true}$) $\vee$ $(l + |L(\mathsf{SK})| > \kappa)$,
Return $\perp$.
$l := l + |L(\mathsf{SK})|$.
Return $L(\mathsf{SK})$.

<u>ENC(M_0, M_1):</u>

$\mathsf{chal} := \mathsf{true}$.
If $|M_0| \neq |M_1|$, Return $\perp$.
$x^* \leftarrow_\$ \mathcal{L}_\rho$ with witness w^*.
$x^* \leftarrow_\$ \mathcal{L}_{\rho_0}$.
$d^* := \mathsf{Pub}(pk_\rho, x^*, w^*) + M_\beta \in \Pi$.
$d^* := \mathsf{Priv}(sk, x^*) + M_\beta \in \Pi$.
$d^* := \mathsf{Priv}(sk', x^*) + M_\beta \in \Pi$.
$d^* \leftarrow_\$ \Pi$.
$\tau^* := \mathsf{H}(x^*, d^*) \in \widetilde{\mathcal{T}}$.
$\widehat{\pi}^* := \widehat{\mathsf{Pub}}(\widehat{pk}_\rho, x^*, w^*) \in \widehat{\Pi}$.
$\widetilde{\pi}^* := \widetilde{\mathsf{Pub}}(\widetilde{pk}_\rho, x^*, w^*, \tau^*) \in \widetilde{\Pi}$.
$\widehat{\pi}^* := \widehat{\mathsf{Priv}}(\widehat{sk}, x^*) \in \widehat{\Pi}$.
$\widetilde{\pi}^* := \widetilde{\mathsf{Priv}}(\widetilde{sk}, x^*, \tau^*) \in \widetilde{\Pi}$.
$\mathcal{Q}_{\mathcal{ENC}} := \mathcal{Q}_{\mathcal{ENC}} \cup \{C^* = (x^*, d^*, \widehat{\pi}^*, \widetilde{\pi}^*)\}$.
$\mathcal{Q}_{\mathcal{TAG}} := \mathcal{Q}_{\mathcal{TAG}} \cup \{\tau^*\}$.
$\Rightarrow C^* := (x^*, d^*, \widehat{\pi}^*, \widetilde{\pi}^*)$.

<u>DEC($C = (x, d, \widehat{\pi}', \widetilde{\pi}')$):</u>

$M := d - \mathsf{Priv}(sk, x) \in \Pi$.
$\tau := \mathsf{H}(x, d) \in \widetilde{\mathcal{T}}$.
$\widehat{\pi} := \widehat{\mathsf{Priv}}(\widehat{sk}, x) \in \widehat{\Pi}$.
$\widetilde{\pi} := \widetilde{\mathsf{Priv}}(\widetilde{sk}, x, \tau) \in \widetilde{\Pi}$.
If $C \notin \mathcal{Q}_{\mathcal{ENC}}$ $\wedge$ $\widehat{\pi}' = \widehat{\pi}$ $\wedge$ $\widetilde{\pi}' = \widetilde{\pi}$
$\wedge$ $\tau \notin \mathcal{Q}_{\mathcal{TAG}}$
$\wedge$ $x \in \mathcal{L}_\rho$,
Return M.
Else,
Return $\perp$.

<u>FINALIZE(β'):</u>

$\Rightarrow (\beta' = \beta)$.

Fig. 16. Games $\mathsf{G}_0 - \mathsf{G}_6$ for the κ-LR-CCA security proof of PKE.

H_0, H_1, H_2, H_3, $\mathsf{H}_{3.i}$, $\mathsf{H}_{3.\lceil \log Q_e \rceil} = \mathsf{H}_4$

INITIALIZE:

$ctr \leftarrow 0.$

$pp \leftarrow_{\$} \mathsf{Setup}(1^\lambda).$

$\widehat{pp} \leftarrow_{\$} \widehat{\mathsf{Setup}}(1^\lambda).$

$\widetilde{pp} \leftarrow_{\$} \widetilde{\mathsf{Setup}}(1^\lambda).$

$(\rho, td) \leftarrow_{\$} \mathscr{L}.$

$(\rho_0, td_0) \leftarrow_{\$} \mathscr{L}_0.$

$\mathsf{H} \leftarrow_{\$} \mathcal{H}.$

$\mathsf{PP} := (pp, \widehat{pp}, \widetilde{pp}, \rho, \mathsf{H}).$

$sk \leftarrow_{\$} \mathcal{SK}.$

$\widehat{sk}, \widehat{sk'} \leftarrow_{\$} \widehat{\mathcal{SK}}.$

$\widetilde{sk}, \widetilde{sk'} \leftarrow_{\$} \widetilde{\mathcal{SK}}.$

$pk_\rho := \alpha_\rho(sk).$

$\widehat{pk}_\rho := \widehat{\alpha}_\rho(\widehat{sk}).$

$\widetilde{pk}_\rho := \widetilde{\alpha}_\rho(\widetilde{sk}).$

$\mathsf{PK} := (pk_\rho, \widehat{pk}_\rho, \widetilde{pk}_\rho).$

$\mathsf{SK} := (sk, \widehat{sk}, \widetilde{sk}).$

$\beta \leftarrow_{\$} \{0, 1\}.$

$l := 0.$

$\mathsf{chal} := \mathsf{false}.$

$\Rightarrow (\mathsf{PP}, \mathsf{PK}).$

LEAK(L):

If $(\mathsf{chal} = \mathsf{true}) \vee (l + |L(\mathsf{SK})| > \kappa)$,

  Return $\perp$.

$l := l + |L(\mathsf{SK})|.$

Return $L(\mathsf{SK})$.

ENC(M_0, M_1):

$\mathsf{chal} := \mathsf{true}.$

If $|M_0| \neq |M_1|$, Return $\perp$.

$ctr \leftarrow ctr + 1.$

$x^* \leftarrow_{\$} \mathcal{L}_{\rho_0}.$

$d^* := \mathsf{Priv}(sk, x^*) + M_\beta \in \Pi.$

$\tau^* := \mathsf{H}(x^*, d^*) \in \widetilde{\mathcal{T}}.$

$\widehat{\pi}^* := \widehat{\mathsf{Priv}}(\widehat{sk}, x^*) \in \widehat{\Pi}.$

$\widehat{\pi}^* := \widehat{\mathsf{Priv}}(\widehat{sk'}, x^*) \in \widehat{\Pi}.$

$\widetilde{\pi}^* := \widetilde{\mathsf{Priv}}(\widetilde{sk}, x^*, \tau^*) \in \widetilde{\Pi}.$

$\widetilde{\pi}^* := \widetilde{\mathsf{Priv}}(\widetilde{sk'}, x^*, \tau^*) \in \widetilde{\Pi}.$

$\widetilde{\pi}^* := \widetilde{\mathsf{Priv}}(\mathsf{RF}_i(ctr_{|i}), x^*, \tau^*).$

$\widetilde{\pi}^* := \widetilde{\mathsf{Priv}}(\mathsf{RF}_{\lceil \log Q_e \rceil}(ctr), x^*, \tau^*).$

$\mathcal{Q}_{\mathcal{ENC}} := \mathcal{Q}_{\mathcal{ENC}} \cup \{C^* = (x^*, d^*, \widehat{\pi}^*, \widetilde{\pi}^*)\}.$

$\mathcal{Q}_{\mathcal{TAG}} := \mathcal{Q}_{\mathcal{TAG}} \cup \{\tau^*\}.$

$\Rightarrow C^* := (x^*, d^*, \widehat{\pi}^*, \widetilde{\pi}^*).$

DEC($C = (x, d, \widehat{\pi}', \widetilde{\pi}')$):

$\tau := \mathsf{H}(x, d) \in \widetilde{\mathcal{T}}.$

If $C \notin \mathcal{Q}_{\mathcal{ENC}} \wedge \tau \notin \mathcal{Q}_{\mathcal{TAG}}$,

  $M := d - \mathsf{Priv}(sk, x) \in \Pi.$

  If $x \in \mathcal{L}_\rho$,

    $\widehat{\pi} := \widehat{\mathsf{Priv}}(\widehat{sk}, x) \in \widehat{\Pi}.$

    $\widetilde{\pi} := \widetilde{\mathsf{Priv}}(\widetilde{sk}, x, \tau) \in \widetilde{\Pi}.$

    If $\widehat{\pi}' = \widehat{\pi} \wedge \widetilde{\pi}' = \widetilde{\pi}$,

      Return M.

  Else If $x \in \mathcal{L}_{\rho_0}$,

    $\widehat{\pi} := \widehat{\mathsf{Priv}}(\widehat{sk}, x) \in \widehat{\Pi}.$

    $\widehat{\pi} := \widehat{\mathsf{Priv}}(\widehat{sk'}, x) \in \widehat{\Pi}.$

    $\widetilde{\pi} := \widetilde{\mathsf{Priv}}(\widetilde{sk}, x, \tau) \in \widetilde{\Pi}.$

    $\widetilde{\pi} := \widetilde{\mathsf{Priv}}(\widetilde{sk'}, x, \tau) \in \widetilde{\Pi}.$

    $\mathcal{S} := \{\widetilde{\pi} := \widetilde{\mathsf{Priv}}(\mathsf{RF}_i(ctr_{|i}), x, \tau) \mid ctr \in [Q_e]\}.$

    $\mathcal{S} := \{\widetilde{\pi} := \widetilde{\mathsf{Priv}}(\mathsf{RF}_{\lceil \log Q_e \rceil}(ctr), x, \tau) \mid ctr \in [Q_e]\}.$

    If $\widehat{\pi}' = \widehat{\pi} \wedge \widetilde{\pi}' = \widetilde{\pi}$,

    If $\widehat{\pi}' = \widehat{\pi} \wedge \widetilde{\pi}' \in \mathcal{S}$,

      $\mathsf{Bad} := \mathsf{true}$ & Return $\perp$.

Return $\perp$.

FINALIZE(β'):

$\Rightarrow \mathsf{Bad}.$

Fig. 17. Hybrids H_0–H_4 for the κ-LR-CCA security proof of PKE.

$\mathsf{H}_{3.i}$, $\mathsf{H}_{3.i.1}$, $\mathsf{H}_{3.i.2}$, $\mathsf{H}_{3.i.3}$, $\mathsf{H}_{3.i.4}$, $\mathsf{H}_{3.i.5}$, $\mathsf{H}_{3.i.6}$

INITIALIZE:

$ctr \leftarrow_\$ 0.$

$pp \leftarrow_\$ \mathsf{Setup}(1^\lambda).$

$\widehat{pp} \leftarrow_\$ \widehat{\mathsf{Setup}}(1^\lambda).$

$\widetilde{pp} \leftarrow_\$ \widetilde{\mathsf{Setup}}(1^\lambda).$

$(\rho, td) \leftarrow_\$ \mathscr{L}.$

$(\rho_0, td_0) \leftarrow_\$ \mathscr{L}_0.$

$(\rho_1, td_1) \leftarrow_\$ \mathscr{L}_1.$

$\mathsf{H} \leftarrow_\$ \mathcal{H}.$

$\mathsf{PP} := (pp, \widehat{pp}, \widetilde{pp}, \rho, \mathsf{H}).$

$sk \leftarrow_\$ \mathcal{SK}.$

$\widehat{sk}, \widehat{sk}' \leftarrow_\$ \widehat{\mathcal{SK}}.$

$\widetilde{sk} \leftarrow_\$ \widetilde{\mathcal{SK}}.$

$pk_\rho := \alpha_\rho(sk).$

$\widehat{pk}_\rho := \widehat{\alpha}_\rho(\widehat{sk}).$

$\widetilde{pk}_\rho := \widetilde{\alpha}_\rho(\widetilde{sk}).$

$\mathsf{PK} := (pk_\rho, \widehat{pk}_\rho, \widetilde{pk}_\rho).$

$\mathsf{SK} := (sk, \widehat{sk}, \widetilde{sk}).$

$\beta \leftarrow_\$ \{0,1\}.$

$l := 0.$

$\mathsf{chal} := \mathsf{false}.$

$\Rightarrow (\mathsf{PP}, \mathsf{PK}).$

LEAK(L):

If $(\mathsf{chal} = \mathsf{true}) \vee (l + |L(\mathsf{SK})| > \kappa)$,

  Return $\perp$.

$l := l + |L(\mathsf{SK})|.$

Return $L(\mathsf{SK})$.

ENC(M_0, M_1):

$\mathsf{chal} := \mathsf{true}.$

If $|M_0| \neq |M_1|$, Return $\perp$.

$ctr \leftarrow_\$ ctr + 1.$

$x^* \leftarrow_\$ \mathcal{L}_{\rho_0}.$

$x^* \leftarrow_\$ \mathcal{L}_{\rho_{ctr_{i+1}}}.$

$d^* := \mathsf{Priv}(sk, x^*) + M_\beta \in \Pi.$

$\tau^* := \mathsf{H}(x^*, d^*) \in \widetilde{\mathcal{T}}.$

$\widehat{\pi}^* := \widehat{\mathsf{Priv}}(\widehat{sk}', x^*) \in \widehat{\Pi}.$

$\widetilde{\pi}^* := \widetilde{\mathsf{Priv}}\big(\mathsf{RF}_i(ctr_{|i}), x^*, \tau^*\big).$

$\widetilde{\pi}^* := \widetilde{\mathsf{Priv}}\big(\mathsf{RF}_{i+1}(ctr_{|i+1}), x^*, \tau^*\big).$

$\mathcal{Q}_{\mathcal{ENC}} := \mathcal{Q}_{\mathcal{ENC}} \cup \{C^* = (x^*, d^*, \widehat{\pi}^*, \widetilde{\pi}^*)\}.$

$\mathcal{Q}_{\mathcal{TAG}} := \mathcal{Q}_{\mathcal{TAG}} \cup \{\tau^*\}.$

$\Rightarrow C^* := (x^*, d^*, \widehat{\pi}^*, \widetilde{\pi}^*).$

DEC$\big(C = (x, d, \widehat{\pi}', \widetilde{\pi}')\big)$:

$\tau := \mathsf{H}(x, d) \in \widetilde{\mathcal{T}}.$

If $C \notin \mathcal{Q}_{\mathcal{ENC}} \wedge \tau \notin \mathcal{Q}_{\mathcal{TAG}}$,

  $M := d - \mathsf{Priv}(sk, x) \in \Pi.$

  If $x \in \mathcal{L}_\rho$,

    $\widehat{\pi} := \widehat{\mathsf{Priv}}(\widehat{sk}, x) \in \widehat{\Pi}.$

    $\widetilde{\pi} := \widetilde{\mathsf{Priv}}(\widetilde{sk}, x, \tau) \in \widetilde{\Pi}.$

    If $\widehat{\pi}' = \widehat{\pi} \wedge \widetilde{\pi}' = \widetilde{\pi}$,

      Return M.

  Else If $x \in \mathcal{L}_{\rho_0} \cup \mathcal{L}_{\rho_1}$,

    $\widehat{\pi} := \widehat{\mathsf{Priv}}(\widehat{sk}', x) \in \widehat{\Pi}.$

    $\mathcal{S} := \big\{\widetilde{\pi} := \widetilde{\mathsf{Priv}}\big(\mathsf{RF}_i(ctr_{|i}), x, \tau\big) \mid ctr \in [Q_e]\big\}.$

    $\mathcal{S} := \big\{\widetilde{\pi} := \widetilde{\mathsf{Priv}}\big(\mathsf{RF}_{i+1}(ctr_{|i} \| d_x), x, \tau\big) \mid ctr \in [Q_e]\big\}.$

    $\mathcal{S} := \big\{\widetilde{\pi} := \widetilde{\mathsf{Priv}}\big(\mathsf{RF}_{i+1}(ctr_{|i} \| b), x, \tau\big) \mid ctr \in [Q_e], b \in \{0,1\}\big\}.$

    $\mathcal{S} := \big\{\widetilde{\pi} := \widetilde{\mathsf{Priv}}\big(\mathsf{RF}_{i+1}(ctr_{|i+1}), x, \tau\big) \mid ctr \in [Q_e]\big\}.$

    If $\widehat{\pi}' = \widehat{\pi} \wedge \widetilde{\pi}' \in \mathcal{S}$,

      $\mathsf{Bad} := \mathsf{true}$ & Return $\perp$.

Return $\perp$.

FINALIZE(β'):

$\Rightarrow \mathsf{Bad}.$

Fig. 18. Hybrids $\mathsf{H}_{3.i}$, $\mathsf{H}_{3.i.1}$–$\mathsf{H}_{3.i.6}$ for the κ-LR-CCA security proof of PKE.

Table of Contents