Hierarchical Identity-Based Encryption with Tight Multi-Challenge Security

Roman Langrehr*[1] and Jiaxin Pan[2]

[1] ETH Zurich, Zurich, Switzerland
roman.langrehr@inf.ethz.ch
[2] Department of Mathematical Sciences
NTNU – Norwegian University of Science and Technology, Trondheim, Norway
jiaxin.pan@ntnu.no

Abstract. We construct the *first* hierarchical identity-based encryption (HIBE) scheme with tight adaptive security in the multi-challenge setting, where adversaries are allowed to ask for ciphertexts for multiple adaptively chosen identities. Technically, we develop a novel technique that can tightly introduce randomness into user secret keys for hierarchical identities in the multi-challenge setting, which cannot be easily achieved by the existing techniques for tightly multi-challenge secure IBE.

In contrast to the previous constructions, the security of our scheme is independent of the number of user secret key queries and that of challenge ciphertext queries. We prove the tight security of our scheme based on the Matrix Decisional Diffie-Hellman Assumption, which is an abstraction of standard and simple decisional Diffie-Hellman assumptions, such as the k-Linear and SXDH assumptions.

Finally, we also extend our ideas to achieve tight chosen-ciphertext security and anonymity, respectively. These security notions for HIBE have not been tightly achieved in the multi-challenge setting before.

Keywords. Hierarchical identity-based encryption, tight security, multi-challenge security, chosen-ciphertext security, anonymity.

1 Introduction

Tight Reductions. In public-key cryptography, most of the schemes are constructed with reduction-based security proofs. A security reduction efficiently maps an adversary $\mathcal{A}$ against the security of a scheme with success probability $\varepsilon_{\mathcal{A}}$ to a solver $\mathcal{B}$ that breaks the hardness of a suitable computational problem with success probability $\varepsilon_{\mathcal{B}}$. We call the quotient $\ell := \varepsilon_{\mathcal{A}}/\varepsilon_{\mathcal{B}}$ the security loss of a reduction, which can be viewed as a quantitative measurement of the distance between the security of the scheme and the hardness of the problem. Ideally, we want (1) the underlying problem to be standard and well-established, (2) the security notion to be realistic, and (3) the security of the scheme to be as close to the hardness of the problem as possible, namely, ℓ to be as close to 1 as possible.

* Parts of the work were done at Karlsruhe Institute of Technology, Karlsruhe, Germany

We consider a reduction *tight* if ℓ is a small constant and the running time of $\mathcal{B}$ is approximately the same as that of $\mathcal{A}$. Many existing works [10,14,15,16] consider a notion of tightness called "almost tight security". Different to the (full) tightness, almost tight security allows the security loss ℓ to be a small polynomial, which is usually a linear function of the security parameter, but still independent of the size of $\mathcal{A}$. We do not distinguish these two notions, but we are precise about the security loss in our comparison tables and security proofs.

Tight reductions are not only theoretically interesting but also beneficial in practice. A tight reduction enables us to give universal key-length recommendations that are independent of the size of an application and shorter than the non-tight ones. This is, in particular, useful in the setting where the envisioned size of an application cannot be reasonably bounded a priori. As a result of that, many recent works have been pursuing efficient tightly secure cryptographic schemes, including digital signature [24,30,16], public-key encryption [14,23,15], identity-based encryption [10,5] schemes, and authenticated key exchange protocols [18].

HIBE meets Tight Security. In this paper, we focus on hierarchical identity-based encryption (HIBE) schemes [28,17]. In an L-level HIBE, an identity is a vector of maximal L identities. It is considered to be more difficult to construct HIBE than IBE and PKE since an HIBE scheme provides more functionalities. For instance, an L-level HIBE scheme allows a user at level $\alpha < L$ to delegate a secret key for its descendants at level $\alpha' > \alpha$.

Constructing tightly secure HIBE appears to be much more challenging. The first tightly secure IBE from standard assumptions was constructed in 2013 [10], while the first tightly secure HIBE was just proposed very recently [32]. We believe that it is not a coincidence. Firstly, Lewko and Waters [37] showed the potential difficulty of constructing tightly secure HIBE. More precisely, they proved that there is a (relatively) large class of HIBE schemes that cannot be tightly proven secure. Secondly, Blazy, Kiltz, and Pan (BKP) [5] made the first attempt to bypass the aforementioned impossibility result. Unfortunately, it has been found that the BKP proof strategy is insufficient for the tight adaptive security of HIBE (cf. [6] and Appendix A of [33]). Adaptive security allows an adversary $\mathcal{A}$ to adaptively choose a challenge identity $\mathsf{id}^\star$ after it sees the master public key and asks for polynomial many user secret keys for identities chosen by $\mathcal{A}$.

Very recently, Langrehr and Pan (LP) proposed the first tightly secure HIBE based on standard assumptions. Their proof strategy improves the one of BKP in the sense that the LP strategy can tightly introduce (suitable) randomness in user secret keys for identities with flexible lengths. Inherently, the LP proof strategy seems to only work tightly in the *single-challenge* setting, where an adversary is restricted to ask for a ciphertext for at most one challenge identity.

From Single- to Multi-Challenge Security. In the real world, an adversary can learn ciphertexts of multiple challenge identities. This is captured by the more realistic multi-challenge security. We note that single-challenge security implies multi-challenge security via a straightforward, but non-tight reduction. This is

mainly the reason why the security of many (H)IBE schemes (e.g. [42,36,35,5,32]) is analyzed in this simple single-challenge setting. However, this straightforward "single- to multi-challenge" reduction loses a relatively large polynomial factor. Namely, if an adversary makes Q_c many queries for challenge ciphertexts, then the overall security loses a factor of Q_c. This defeats the purpose of establishing tight reductions for the overall scheme in a more realistic setting.

Our Goal: HIBE with Tight Multi-Challenge Security. We aim at constructing tightly secure HIBE schemes in the more realistic multi-challenge setting. We note that there exist several techniques in constructing tightly multi-challenge secure IBE schemes (for instance, [27,20,21,25]) in composite- or prime-order pairing groups. However, as already observed by the LP paper, these techniques cannot be easily used in the HIBE setting. Thus, to achieve our goal, it requires us to develop a new technique for tight multi-challenge security that is useful for HIBE schemes.

1.1 Our Contribution

We construct the *first* tightly chosen-plaintext secure HIBE schemes in the multi-challenge setting. The main novelty of this paper is a new randomization technique that enables us to randomize user secret keys for hierarchical identities in the multi-challenge setting. We highlight that our technique improves the existing techniques [27,20,21,25] for tightly multi-challenge secure IBE schemes in the sense that ours can handle randomization for identities with flexible lengths. We postpone the detailed comparison of these techniques in Section 1.3.

Following the "MAC-to-(H)IBE" framework [5,32], we capture our core technique with the notion of affine MACs with levels (which was firstly proposed in [32]) in the multi-challenge setting. By using prime-order pairings and the Matrix Decisional Diffie-Hellman (MDDH) assumption [13], we compile any of these MAC schemes to an HIBE tightly in the multi-challenge setting. We have two main constructions of the affine MACs, MAC_1 and MAC_2, and they give us two HIBE with different advantages and disadvantages, respectively: Considering identity space $\mathcal{ID} := (\{0,1\}^n)^{\leq L}$, our first scheme has constant amount of group elements in the ciphertext, but $\mathbf{O}(nL)$ many elements in the user secret key; and our second scheme has shorter user secret key that contains $\mathbf{O}(L)$ many elements, but its ciphertext contains $\mathbf{O}(L)$ many elements. Both schemes have security loss $\mathbf{O}(n \cdot L^2)$ and independent of the numbers of challenge ciphertext queries and user secret key queries. Table 1 compares our schemes with the existing HIBE schemes in prime-order pairing groups.

We extend our main results in the following directions by using known techniques:

Anonymity. Additionally, the first construction of our MACs, MAC_1, has tight anonymity. By using the anonymity-preserving transformation of [5], we construct the *first* tightly secure, anonymous HIBE scheme in the multi-challenge setting. An (H)IBE scheme is anonymous if its challenge ciphertexts hide the corresponding identities. An application of anonymous HIBE is PKE with keyword search [1].

Scheme	$\lvert\mathsf{mpk}\rvert$	$\lvert\mathsf{usk}\rvert$	$\lvert\mathsf{C}\rvert$	Loss	MC	Ass.
Wat05 [42]	$\mathbf{O}(nL)\lvert\mathbb{G}\rvert$	$\mathbf{O}(nL)\lvert\mathbb{G}\rvert$	$(1+p)\lvert\mathbb{G}\rvert$	$\mathbf{O}(nQ_\mathsf{e})^L$	✗	DBDH
Wat09 [41]	$\mathbf{O}(L)\lvert\mathbb{G}\rvert$	$\mathbf{O}(p)(\lvert\mathbb{G}\rvert+\lvert\mathbb{Z}_q\rvert)$	$\mathbf{O}(p)(\lvert\mathbb{G}\rvert+\lvert\mathbb{Z}_q\rvert)$	$\mathbf{O}(Q_\mathsf{e})$	✗	2-LIN
Lew12 [35]	$60\lvert\mathbb{G}\rvert+2\lvert\mathbb{G}_T\rvert$	$(60+10p)\lvert\mathbb{G}\rvert$	$10p\lvert\mathbb{G}\rvert$	$\mathbf{O}(Q_\mathsf{e}L)$	✗	2-LIN
CW13 [10]	$\mathbf{O}(Lk^2)(\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert)$	$\mathbf{O}(Lk)\lvert\mathbb{G}_2\rvert$	$(2k+2)\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(Q_\mathsf{e})$	✗	k-LIN
BKP14 [5]	$\mathbf{O}(Lk^2)(\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert)$	$\mathbf{O}(Lk)\lvert\mathbb{G}_2\rvert$	$(2k+2)\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(Q_\mathsf{e})$	✗	k-LIN
GCTC16 [19]	$(6k^2+12k)(\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert)$ $+(k+2)\lvert\mathbb{G}_T\rvert$	$((6k+12)\lceil p/3\rceil$ $-(k+2)p)\lvert\mathbb{G}_2\rvert$	$(3k+6)\lceil p/3\rceil\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(QL)$	✗	k-LIN
$\mathsf{LP19}_1$ [32]	$\mathbf{O}(nL^2k^2)(\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert)$	$\mathbf{O}(nL^2k)\lvert\mathbb{G}_2\rvert$	$(4k+1)\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(nL^2k)$	✗	k-LIN
$\mathsf{LP19}_1^{\mathcal{H}}$ [32]	$\mathbf{O}(\gamma Lk^2)(\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert)$	$\mathbf{O}(\gamma Lk)\lvert\mathbb{G}_2\rvert$	$(4k+1)\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(\gamma Lk)$	✗	k-LIN
$\mathsf{LP19}_2$ [32]	$\mathbf{O}(nL^2k^2)(\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert)$	$(3kp+k+1)\lvert\mathbb{G}_2\rvert$	$(3kp+k+1)\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(nLk)$	✗	k-LIN
$\mathsf{LP19}_2^{\mathcal{H}}$ [32]	$\mathbf{O}(\gamma Lk^2)(\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert)$	$(3kp+k+1)\lvert\mathbb{G}_2\rvert$	$(3kp+k+1)\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(\gamma k)$	✗	k-LIN
HIBKEM_1	$\mathbf{O}(nL^2k^2)(\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert)$	$\mathbf{O}(nL^2k)\lvert\mathbb{G}_2\rvert$	$5k\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(nL^2k)$	✓	k-LIN
$\mathsf{HIBKEM}_1^{\mathcal{H}}$	$\mathbf{O}(\gamma Lk^2)(\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert)$	$\mathbf{O}(\gamma Lk)\lvert\mathbb{G}_2\rvert$	$5k\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(\gamma Lk)$	✓	k-LIN
HIBKEM_2	$\mathbf{O}(nL^2k^2)(\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert)$	$(3kp+2k)\lvert\mathbb{G}_2\rvert$	$(3kp+2k)\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(nLk)$	✓	k-LIN
$\mathsf{HIBKEM}_2^{\mathcal{H}}$	$\mathbf{O}(\gamma Lk^2)(\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert)$	$(3kp+2k)\lvert\mathbb{G}_2\rvert$	$(3kp+2k)\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(\gamma k)$	✓	k-LIN

Table 1. Comparison of HIBEs in prime-order pairing groups with adaptive security in the standard model based on static assumptions. The highlighted rows are from this paper. HIBKEM_1 can be found in Figure 40, and HIBKEM_2 can be found in Figure 41. The schemes with $\mathcal{H}$ in the superscript are obtained by hashing the identities as described in the full version of [32].

The hierarchical identity space is $(\{0,1\}^n)^{\leq L}$, and γ is the bit length of the range of a collision-resistant hash function. '$\lvert\mathsf{mpk}\rvert$,' '$\lvert\mathsf{usk}\rvert$,' and '$\lvert\mathsf{C}\rvert$' stand for the size of the master public key, a user secret key and a ciphertext, respectively. We count the number of group elements in $\mathbb{G}_1, \mathbb{G}_2$, and $\mathbb{G}_T$. For a scheme that works in symmetric pairing groups, we write $\mathbb{G}(:= \mathbb{G}_1 = \mathbb{G}_2)$. The schemes that work in asymmetric pairing groups can be instantiated with SXDH=1-LIN. In the '$\lvert\mathsf{usk}\rvert$' and '$\lvert\mathsf{C}\rvert$' columns p stands for the hierarchy depth of the identity vector. In bounded HIBEs, L denotes the maximum hierarchy depth. In the security loss, Q_e denotes the number of user secret key queries by the adversary. The last but one column indicates whether the adversary is allowed to query multiple challenge ciphertexts (✓) or just one (✗). The last column shows the underlying security assumption.

We note that it was unknown how to construct a tightly adaptively secure anonymous HIBE scheme even in the single-challenge setting.

Chosen-Ciphertext Security. We note that ciphertexts of our HIBE schemes have compatible structure to use Quasi-Adaptive Non-Interactive Zero-Knowledge (QANIZK) argument for linear subspace systems [29,31,25,2]. Similar to [25], we upgrade our schemes to chosen-ciphertext security by using any tightly unbounded simulation-sound QANIZK scheme. These schemes are the first tightly chosen-ciphertext secure HIBE schemes in the multi-challenge setting. Combining with the technique in the first extension, we also construct a tightly chosen-ciphertext secure and anonymous HIBE.

More (Minor) Extensions. Additionally, our schemes have tight multi-instance security. In the multi-instance setting, an adversary can get multiple instances of the HIBE scheme. It is trivial that our HIBE schemes are tightly secure in this setting, since, given an instance of our HIBE, it can be easily rerandomized to get multiple instances from it.

In the full version of [32], they use a collision-resistant hash function to further improve the security loss and master public key size of their schemes. Here we can also do the same improvement.

These two extensions are rather minor and we skip the technical details here, but include them in Table 1 for a more complete comparison of different HIBE schemes.

1.2 Technical Details

We give an overview of our main technique in achieving tight adaptive security for HIBE in the multi-challenge setting. Here we restrict ourselves to chosen-plaintext security.

Starting Point: The BKP Framework. To set up the stage of our discussion, we recall the BKP framework [5], which transforms an algebraic MAC scheme to an IBE scheme in prime-order pairing groups. The algebraic MAC is called affine MAC, due to its affine structure. Their framework is an abstraction of the Chen-Wee (CW) IBE [10] and can also be viewed as an extension of the "MAC-to-Signature" framework by Bellare and Goldwasser (BG) [4] in the IBE context. In particular, the BKP framework can be viewed as a fine-grained reverse of the Naor transformation [7] on the BG signature scheme.

We give some informal ideas about how an affine MAC can be turned into an IBE. The master public key of an IBE, $\mathsf{pk} := \mathsf{Com}(\mathsf{sk}_{\mathsf{MAC}})$, is a commitment of the MAC secret key, $\mathsf{sk}_{\mathsf{MAC}}$. A user secret key $\mathsf{usk}[\mathsf{id}]$ of an identity id consists of a BG signature, namely, a MAC tag τ_{id} on the message id and a NIZK proof of the validity of τ_{id} w.r.t. the secret key committed in pk. The observation of BKP is that one can implement these commitments and NIZK proofs with the (tuned) Groth-Sahai proof system [22].

Due to the fact that the BKP MAC has affine structures, the NIZK verification involves only linear equations and can be randomized. Indeed, the BKP IBE ciphertext C_{id} can be viewed as a randomized linear combination of pk w.r.t. id. Implicitly, the decryption algorithm is a randomized NIZK verification of the validity of τ_{id} (from $\mathsf{usk}[\mathsf{id}]$): If τ_{id} is valid, then the ciphertext C_{id} can be correctly decrypted.

Obstacles in Achieving our Goal with BKP. The BKP framework has a nice property that the security of the IBE scheme can be tightly reduced to the security of the MAC scheme. Thus, we can only focus on constructing tightly secure MAC, which is more fundamental. In particular, the BKP framework has a tightly secure MAC scheme $\mathsf{MAC}_{\mathsf{NR}}$ in the single-challenge setting under a standard assumption. $\mathsf{MAC}_{\mathsf{NR}}$ is implicitly in the CW IBE and borrows some idea from the Naor-Reingold PRF [38]. However, $\mathsf{MAC}_{\mathsf{NR}}$ has limitations that

(a) it can only be used to handle at most one IBE challenge ciphertext, and
(b) it cannot provide tight adaptive security for HIBE.

We recall $\mathsf{MAC_{NR}}$ and give more technical discussion about these two limitations.

Let $\mathbb{G}_2 := \langle P_2 \rangle$ be an additive prime-order group. We use the implicit notation $[x]_2 := xP_2$ as in [13]. $\mathsf{MAC_{NR}}$ chooses $\mathbf{B} \in \mathbb{Z}_q^{(k+1)\times k}$ according to the underlying assumption. $\mathbf{B}$ always has rank k and, for simplicity, we assume that the first k rows of $\mathbf{B}$, denoted by $\overline{\mathbf{B}}$, forms a full-rank square matrix. For message space $\mathcal{M} := \{0,1\}^n$, which is the same as the identity space of the resulting IBE, its secret key is chosen uniformly at random and has the form of

$$\mathsf{sk_{MAC}} := \left((\mathbf{x}_{i,b})_{1\le i\le n, b\in\{0,1\}}, x'_0 \right) \in \left(\mathbb{Z}_q^{k\cdot 2}\right)^n \times \mathbb{Z}_q \,.$$

Its MAC tag $\tau := ([\mathbf{t}]_2, [u]_2)$ contains a random vector $[\mathbf{t}]_2$ and a message-dependent value $[u]_2$ in the form of

$$\begin{aligned} \mathbf{t} &= \overline{\mathbf{B}}\mathbf{s} \in \mathbb{Z}_q^k \qquad \text{for random } \mathbf{s} \in \mathbb{Z}_q^k \\ u &= \textstyle\sum_i \mathbf{x}_{i,\mathsf{m}_i}^\top \mathbf{t} + x'_0 \in \mathbb{Z}_q. \end{aligned} \tag{1}$$

Based on the MDDH assumption, $\mathsf{MAC_{NR}}$ is tightly pseudorandom against chosen-message attacks ($\mathsf{PR\text{-}CMA}$ security), which is a decisional variant of the standard existential unforgeability against chosen-message attacks ($\mathsf{EUF\text{-}CMA}$ security) for MAC schemes [11]. Essentially, the $\mathsf{PR\text{-}CMA}$ security of $\mathsf{MAC_{NR}}$ shows that $[u]_2$ is pseudorandom.

To understand the intuition of the BKP proof strategy, we consider the standard $\mathsf{EUF\text{-}CMA}$ security, where an adversary $\mathcal{A}$ can ask for polynomial many MAC tags $\tau_\mathsf{m} := ([\mathbf{t}_\mathsf{m}]_2, [u_\mathsf{m}]_2)$ on messages m of its adaptive choice and submit a forgery $\tau^\star := ([\mathbf{t}^\star]_2, [u^\star]_2)$ for *one single* verification. The MAC tag query is corresponding to the IBE user secret key query, and the verification query is related to the IBE challenge ciphertext query.

The overall proof strategy of $\mathsf{MAC_{NR}}$ is to gradually randomize all the u values in answering $\mathcal{A}$'s tag queries. During this process, the reduction must be able to compute $u^\star = \sum_i \mathbf{x}_{i,\mathsf{m}_i^\star}^\top \mathbf{t}^\star + x'_0$ for a fresh $\mathsf{m}^\star$, which is the main difficulty in the proof. To solve it, the BKP argument conceptually replace x'_0 with a constant random function $\mathsf{RF}_0(\varepsilon)$. Then, by using the MDDH assumption, it develops a random function $\mathsf{RF}_{i+1} : \{0,1\}^{i+1} \to \mathbb{Z}_q$ from another random function $\mathsf{RF}_i : \{0,1\}^i \to \mathbb{Z}_q$ on-the-fly for some integer $0 \le i < n$. After n recursions, a random function $\mathsf{RF} : \{0,1\}^n \to \mathbb{Z}_q$ is developed and thus the security loss of $\mathsf{MAC_{NR}}$ is $\mathbf{O}(n)$. More precisely, in each step, the reduction guesses the $(i+1)$-th bit of $\mathsf{m}^\star$ as $b^\star \in \{0,1\}$ and defines the function RF_{i+1} as:

$$\mathsf{RF}_{i+1}(\mathsf{m}_{|i+1}) := \begin{cases} \mathsf{RF}_i(\mathsf{m}_{|i}) & (\text{if } \mathsf{m}_{i+1} = b^\star) \\ \mathsf{RF}_i(\mathsf{m}_{|i}) + R_{\mathsf{m}_{|i}} & (\text{if } \mathsf{m}_{i+1} = 1 - b^\star) \end{cases}, \tag{2}$$

where $\mathsf{m}_{|i}$ is the first i bits of m and $R_{\mathsf{m}_{|i}}$ is a random value from $\mathbb{Z}_q$ chosen for $\mathsf{m}_{|i}$. Alternatively, the BKP strategy can be viewed as gradually injecting randomness directly into x'_0, during developing the random function above.

There are two important observations of this strategy, which lead to Limitations (a) and (b) above. These observations are in the proof step from Hybrid i (using RF_i) to Hybrid $(i+1)$ (using RF_{i+1}):

Reason for Limitation (a): In this step, the reduction embeds a MDDH problem instance in $[\mathbf{x}_{i+1,1-b^\star}]_2$ and chooses the other $\mathbf{x}_{j,b}$ in $\mathbb{Z}_q$. Thus, $\mathbf{x}_{i+1,1-b^\star}$ in $\mathbb{Z}_q$ is unknown to the reduction during this step, but $\mathbf{x}_{i+1,b^\star}$ is known in $\mathbb{Z}_q$ for verifying the forgery on a single $\mathsf{m}^\star$. However, this strategy cannot work tightly if there is more than one verification queries, which is required in the multi-challenge setting. For instance, after guessing $b^\star$, the reduction fails to answer two verification queries for challenge messages, 0^n and 1^n, respectively.

Reason for Limitation (b): RF_{i+1} defined via Equation (2) is a random function for message spaces with fixed length based on the crucial fact that the outputs of RF_{i+1} and RF_i are not revealed at the same time. However, for hierarchical identity spaces, $\mathcal{ID} := (\{0,1\}^n)^{\leq L}$, it is not the case anymore.

As a concrete example, we consider the transition from Hybrids n to $(n+1)$. Via Equation (2), $\mathsf{RF}_n(\mathsf{m}) = \mathsf{RF}_{n+1}(\mathsf{m}||b^\star)$ and adversaries can learn this by asking MAC tags for m and $\mathsf{m}||b^\star||\mathsf{m}'$ (where $\mathsf{m}' \in \{0,1\}^{n-1}$). Thus, the tags for these two message are not independent and we cannot continue the hybrid argument.

In order to solve our task, we need to develop new techniques to overcome both limitations described above. Our approach essentially has two main steps: In the first step, we target at tight multi-challenge security, and, at the same time, we are looking ahead and making it suitable for handling hierarchical identities; and, in the second step, we upgrade the technique developed in the first step to the HIBE setting.

Step 1: New Strategy for Tight Multi-Challenge Security. We call this randomization strategy subspace randomization, since it first increases the dimension of $\mathbf{t}$ in the tag so that there exist subspaces, and our crucial randomization happens in some of these subspaces. This subspace randomization is compatible with the independent randomization of Langrehr and Pan [32] and, thus, it gets extended in Step 2 to randomize MAC tags for messages with flexible length, namely, hierarchical identities.

Our starting point of achieving tight multi-challenge security is to design a new randomization strategy that does not depend on any bit of $\mathsf{m}^\star$. To implement this strategy, our first attempt is to choose the random vector $\mathbf{t}$ in the MAC tag from a larger vector space $\mathbb{Z}_q^{2k}$. Accordingly, we choose $\mathbf{x}_{j,b}$ values in $\mathsf{sk}_{\mathsf{MAC}}$ from $\mathbb{Z}_q^{2k}$ and compute $([\mathbf{t}]_2, [u]_2)$ in the MAC tag as

$$\begin{aligned} &\mathbf{t} \xleftarrow{\$} \mathbb{Z}_q^{2k} \\ &u = \sum\nolimits_i \mathbf{x}_{i,\mathsf{m}_i}^\top \mathbf{t} + x_0' \in \mathbb{Z}_q. \end{aligned} \tag{3}$$

Our proof strategy is rather algebraic and make use of some simple facts about the vector space $\mathbb{Z}_q^{2k}$. We choose two random matrices $\mathbf{B}_0, \mathbf{B}_1 \xleftarrow{\$} \mathbb{Z}_q^{2k\times k}$ and $\mathbf{B}_0^\perp, \mathbf{B}_1^\perp \in \mathbb{Z}_q^{2k\times k}$ are the corresponding non-zero kernel matrices, respectively.

Namely,

$$\mathbf{B}_0^\top \cdot \mathbf{B}_0^\perp = \mathbf{B}_1^\top \mathbf{B}_1^\perp = \mathbf{0} \in \mathbb{Z}_q^{k \times k} \tag{4}$$

$(\mathbf{B}_0 \mid \mathbf{B}_1)$ is a basis of $\mathbb{Z}_q^{2k}$. $\mathsf{Span}(\mathbf{B}_0) := \{\mathbf{v} \in \mathbb{Z}_q \mid \exists \mathbf{w} \in \mathbb{Z}_q^k \text{ s.t. } \mathbf{v} = \mathbf{B}_0 \cdot \mathbf{w}\}$ is a linear subspace of $\mathbb{Z}_q^{2k}$ and it is the same for $\mathsf{Span}(\mathbf{B}_1)$.

We note that in the value u the information of the secret $\mathbf{x}_{j,b}$ values is only projected to $\mathbf{t}$. When we answer a tag query on message m, we can switch $\mathbf{t}$ to a suitable subspace (either $\mathsf{Span}(\mathbf{B}_0)$ or $\mathsf{Span}(\mathbf{B}_1)$) by the MDDH assumption. After the switch, some information about $\mathbf{x}_{j,b}$ values is perfectly hidden, and we can use it to gradually randomize the u values. Choosing $\mathbf{t}$ from the suitable subspace depends on the corresponding bit of m, but independent of the guess of $\mathsf{m}^\star$.

More precisely, in our Hybrid i, for a tag query on m, our u_m has the form

$$u_\mathsf{m} := \Big(\sum\nolimits_j \mathbf{x}_{j,\mathsf{m}_j}^\top + \underbrace{\mathsf{OF}_i(\mathsf{m}_{|i})(\mathbf{B}_0^\perp)^\top + \mathsf{ZF}_i(\mathsf{m}_{|i})(\mathbf{B}_1^\perp)^\top}_{=:\mathsf{RF}_i(\mathsf{m}_{|i})} \Big) \mathbf{t}_\mathsf{m} + x_0' \,,$$

where $\mathsf{OF}_i, \mathsf{ZF}_i : \{0,1\}^i \to \mathbb{Z}_q^{1 \times k}$ are two independent random functions. Since $(\mathbf{B}_0^\perp \mid \mathbf{B}_1^\perp)^\top \in \mathbb{Z}_q^{2k \times 2k}$ is full-rank with overwhelming probability, we can view $\big(\mathsf{OF}_i(\mathsf{m}_{|i}) \mid \mathsf{ZF}_i(\mathsf{m}_{|i})\big)(\mathbf{B}_0^\perp \mid \mathbf{B}_1^\perp)^\top$ as a random function $\mathsf{RF}_i : \{0,1\}^i \to \mathbb{Z}_q^{1 \times 2k}$.

In the transition to Hybrid $(i+1)$, we do the following two sub-steps:

- Step 1.1 (using MDDH): If $\mathsf{m}_{i+1} = 0$, then we choose $\mathbf{t}_\mathsf{m}$ from $\mathsf{Span}(\mathbf{B}_0)$, otherwise, from $\mathsf{Span}(\mathbf{B}_1)$.
- Step 1.2 (information-theoretic argument): For all tag queries with $\mathsf{m}_{i+1} = 0$, we increase the entropy in OF_i and develop OF_{i+1}. By Equation (4), this change is perfectly hidden from the adversary $\mathcal{A}$. Similarly, we also develop ZF_{i+1} from ZF_i.

Now we can introduce RF_{i+1} and, after n of these recursions, we can have RF_n to randomize all the tags.

The only thing left is to handle multiple verification queries. To this end, in our scheme, we choose random $\mathbf{X}_{j,b} \in \mathbb{Z}_q^{k \times 2k}$. Compared with $\mathbf{x}_{j,b}^\top \in \mathbb{Z}_q^{2k}$, our new $\mathbf{X}_{j,b}$ has more rows such that we can embed the MDDH challenge to randomize multiple verification queries as well. We do not always know all the whole $\mathbf{X}_{j,b}$ values over $\mathbb{Z}_q$. However, different to the BKP or CW strategy, we multiply the unknown part in $\mathbf{X}_{j,b}$ with the suitable kernel matrix, either $\mathbf{B}_0^\perp$ or $\mathbf{B}_1^\perp$. This is done implicitly. Since, in all the tag queries, $\mathbf{t}_\mathsf{m}$ has already been chosen in the correct subspace, the unknown part will not appear, and we can simulate the tag queries. When we answer the verification queries, this unknown part will "react with" these queries and randomize them, which will later be the challenge ciphertext queries of the resulting IBE.

To sum up the discussion above, our strategy increases the dimension of $\mathbf{x}_{j,b}^\top \in \mathbb{Z}_q^{1 \times k}$ to $\mathbf{X}_{j,b} \in \mathbb{Z}_q^{k \times 2k}$ in such a way that we have enough entropy from the row vectors to randomize tag queries and, combining it with the entropy from the column vectors, we can handle the verification queries at the same time.

We capture all the above discussion formally by presenting an affine MAC in Section 3.1, which can be used to construct a tightly multi-challenge secure IBE.

We are not claiming any efficiency improvement with this IBE, but technical achievement, instead, since it has roughly the same efficiency as its counterparts from [20,21,25]. However, our techniques involved in this IBE scheme improves those in [20,21,25] in the sense that ours can be extended to randomize user secret keys for hierarchical identities, while those in [20,21,25] cannot.

Step 2: Upgrade to Hierarchical Identities. For the random function RF_i developed via the strategy above, an important observation is that its output is only projected in $\mathbf{t}$ during the hybrid argument. This gives us "room" to upgrade the subspace randomization to handle hierarchical identities: By controlling the choice of $\mathbf{t}$, we can make sure that the outputs of RF_i and RF_{i+1} will not appear at the same time via the value u.

The strategy in this step is motivated by the work of Langrehr and Pan [32], where their core technique is to isolate the randomization for messages at different levels (which will be identities at different levels in the HIBE). To implement this, we add a "layer" to $\mathbf{t}$ by choosing $\mathbf{t}$ from $\mathbb{Z}_q^{3k}$. Similar to Step 1, we exploit some properties of the linear space $\mathbb{Z}_q^{3k}$. We choose two random matrices $\mathbf{B}_0, \mathbf{B}_1 \xleftarrow{\$} \mathbb{Z}_q^{3k\times k}$ and decompose $\mathbb{Z}_q^{3k}$ into $\mathsf{Span}(\mathbf{B} \mid \mathbf{B}_0 \mid \mathbf{B}_1)$. The span of $\mathbf{B}^\perp$ is decomposed into that of $\mathbf{B}_0^* \in \mathbb{Z}_q^{3k\times k}$ and $\mathbf{B}_1^* \in \mathbb{Z}_q^{3k\times k}$. An overview of the orthogonal relations between all these matrices is given in Figure 1.

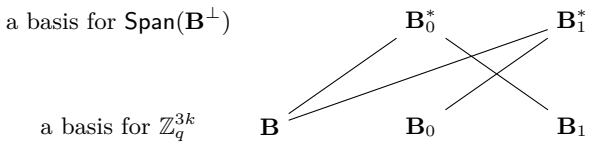


Fig. 1. Solid lines mean orthogonal: $\mathbf{B}^\top\mathbf{B}_0^* = \mathbf{B}_1^\top\mathbf{B}_0^* = \mathbf{0} = \mathbf{B}^\top\mathbf{B}_1^* = \mathbf{B}_0^\top\mathbf{B}_1^* \in \mathbb{Z}_q^{k\times k}$.

The intuition of our technique is that we develop a random function in $\mathsf{Span}(\mathbf{B}^\perp)$, which is orthogonal to $\mathsf{Span}(\mathbf{B})$. Thus, it is easy to isolate the randomization for messages at level $\alpha(\leq L)$[3] from that at other levels by choosing $\mathbf{t}_\mathsf{m}$ from $\mathsf{Span}(\mathbf{B})$ for $\mathsf{m} \in (\{0,1\}^n)^{\alpha'}$ and $\alpha' \neq \alpha$. The randomization with a level α is done similar to Step 1. In particular, $(\mathbf{B}_0, \mathbf{B}_1^*)$ functions similar to $(\mathbf{B}_0, \mathbf{B}_0^\perp)$ in Step 1, and the same for $(\mathbf{B}_1, \mathbf{B}_0^*)$ vs. $(\mathbf{B}_1, \mathbf{B}_1^\perp)$.

We only present our intuitions here and refer Section 3.2 and Appendix B for the actual constructions and formal proofs.

1.3 More on Related Works

As we discussed before, there are different techniques [3,27,20,21,25] to achieve tight multi-challenge security for IBE schemes. Schemes in [21,25] are based on

[3] For message space with flexible length $\mathcal{M} := (\{0,1\}^n)^{\leq L}$, a message at level α means $\mathsf{m} \in (\{0,1\}^n)^\alpha$.

the BKP framework and close to ours, while the other schemes are either using composite-order pairings [27] or based on stronger, non-standard assumptions [3,20]. We suppose the proof strategy in the work of Hofheinz, Jia, and Pan (HJP) [25] cannot be easily extended to randomize MAC tags for hierarchical identities, since their technique develops the random function RF_i in the full space $\mathbb{Z}_q$ and directly introduce randomness into x'_0. Inherently, in the HIBE setting, this strategy has the same limitation as BKP, namely, the outputs of RF_i and RF_{i+1} are both leaked when identities have different lengths. The work of Gong et al. [21] has the same issue as well. This limitation explains why some proof steps of LP HIBE schemes cannot be done in the multi-challenge setting, even with the HJP technique.

1.4 Open Problems

As mentioned before and observed in Table 1, the tighter security loss of our schemes is $\mathbf{O}(\gamma k)$, but with relatively larger ciphertext. We leave further improving the security loss with compact ciphertext as an open problem.

Another interesting direction is to make our schemes more efficient. A main disadvantage of our schemes is that they require relatively large master public keys. More precisely, ignoring the small constant k, mpk contains either $\mathbf{O}(\alpha L^2)$ or $\mathbf{O}(\gamma L)$ group elements, because of the use of the LP technique [32]. An interesting open problem is to construct a tightly secure HIBE with shorter master public keys, probably first in the single-challenge setting. A similar interesting open problem is to shorten the size of either user secret keys or ciphertexts to have a more efficient, tightly secure HIBE scheme in the multi-challenge setting.

1.5 Roadmap

We recall useful definitions in Section 2. Section 3 proposes affine MACs that can be used to construct tightly multi-challenge secure IBE and HIBE, respectively. It presents our core techniques as described above in a detailed and formal manner. Appendix C constructs an affine MAC, which is anonymous and can be used to construct anonymous HIBE. Appendix D transforms our MAC schemes to CPA- and CCA-secure HIBE schemes, respectively, based on the frameworks from [5,25]. Appendix E transforms our anonymous MAC to anonymous CPA- and CCA-secure HIBE schemes, respectively. Appendix F gives concrete instantiations of our schemes. For readers only interested in our core techniques, we refer Section 3 to them, and other sections are for completeness of our claims.

2 Preliminaries

Notations. We use $x \xleftarrow{\$} \mathcal{S}$ to denote the process of sampling an element x from $\mathcal{S}$ uniformly at random if $\mathcal{S}$ is a set and to denote the process of running $\mathcal{S}$ with its internal randomness and assign the output to x if $\mathcal{S}$ is an algorithm. The expression

$a \stackrel{?}{=} b$ stands for comparing a and b on equality and returning the result in Boolean value. For positive integers $k, \eta \in \mathbb{N}_+$ and a matrix $\mathbf{A} \in \mathbb{Z}_q^{(k+\eta)\times k}$, we denote the upper square matrix of $\mathbf{A}$ by $\overline{\mathbf{A}} \in \mathbb{Z}_q^{k\times k}$ and the lower η rows of $\mathbf{A}$ by $\underline{\mathbf{A}} \in \mathbb{Z}_q^{\eta\times k}$. Similarly, for a column vector $\mathbf{v} \in \mathbb{Z}_q^{k+\eta}$, we denote the upper k elements by $\overline{\mathbf{v}} \in \mathbb{Z}_q^k$ and the lower η elements of $\mathbf{v}$ by $\underline{\mathbf{v}} \in \mathbb{Z}_q^\eta$. We use $\mathbf{A}^{-\top}$ as shorthand for $\left(\mathbf{A}^{-1}\right)^\top$. For a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, we use $\mathsf{Span}(\mathbf{A}) := \left\{\mathbf{A}\mathbf{v} \mid \mathbf{v} \in \mathbb{Z}_q^m\right\}$ to denote the linear span of $\mathbf{A}$ and $\mathbf{A}^\perp$ denotes an arbitrary matrix with $\mathsf{Span}\left(\mathbf{A}^\perp\right) = \left\{\mathbf{v} \mid \mathbf{A}^\top\mathbf{v} = \mathbf{0}\right\}$.

For a set $\mathcal{S}$ and $n \in \mathbb{N}_+$, $\mathcal{S}^n$ denotes the set of all n-tuples with components in $\mathcal{S}$. For a string $\mathsf{m} \in \Sigma^n$, m_i denotes the i-th component of m ($1 \le i \le n$) and $\mathsf{m}_{|i}$ denotes the prefix of length i of m. Furthermore for a p-tuple of bit strings $\mathsf{m} \in (\{0,1\}^n)^p$, we use $[\![\mathsf{m}]\!]$ to denote the string $\mathsf{m}_1||\ldots||\mathsf{m}_p$. Thus for $1 \le i \le np$, $[\![\mathsf{m}]\!]_i$ denotes the i-th bit of $\mathsf{m}_1||\ldots||\mathsf{m}_p$ and $[\![\mathsf{m}]\!]_{|i}$ denotes the i-bit-long prefix of $\mathsf{m}_1||\ldots||\mathsf{m}_p$.

All algorithms in this paper are probabilistic polynomial-time unless we state otherwise. If $\mathcal{A}$ is an algorithm, then we write $a \xleftarrow{\$} \mathcal{A}(b)$ to denote the random variable outputted by $\mathcal{A}$ on input b.

Games. Following [5], we use code-based games to define and prove security. A game G contains procedures Init and Finalize, and some additional procedures $\mathrm{P}_1, \ldots, \mathrm{P}_n$, which are defined in pseudo-code. Initially all variables in a game are undefined (denoted by $\perp$), all sets are empty (denote by $\emptyset$), and all partial maps (denoted by $f : A \dashrightarrow B$) are totally undefined. An adversary $\mathcal{A}$ is executed in game G (denote by $\mathsf{G}^{\mathcal{A}}$) if it first calls Init, obtaining its output. Next, it may make arbitrary queries to P_i (according to their specification), again obtaining their output. Finally, it makes one single call to Finalize($\cdot$) and stops. We use $\mathsf{G}^{\mathcal{A}} \Rightarrow d$ to denote that G outputs d after interacting with $\mathcal{A}$, and d is the output of Finalize.

$T(\mathcal{A})$ denotes the running time of $\mathcal{A}$.

2.1 Pairing Groups and Matrix Diffie-Hellman Assumptions

Let GGen be a probabilistic polynomial-time (PPT) algorithm that on input 1^λ returns a description $\mathcal{G} := (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$ of asymmetric pairing groups where $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$ are cyclic groups of order q for a λ-bit prime q. The group elements P_1 and P_2 are generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. The function $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is an efficient computable (non-degenerated) bilinear map. Define $P_T := e(P_1, P_2)$, which is a generator in $\mathbb{G}_T$. In this paper, we only consider Type III pairings, where $\mathbb{G}_1 \neq \mathbb{G}_2$ and there is no efficient homomorphism between them. All constructions in this paper can be easily instantiated with Type I pairings by setting $\mathbb{G}_1 = \mathbb{G}_2$ and defining the dimension k to be greater than 1.

We use the implicit representation of group elements as in [13]. For $s \in \{1, 2, T\}$ and $a \in \mathbb{Z}_q$ define $[a]_s = aP_s \in \mathbb{G}_s$ as the implicit representation of a in $\mathbb{G}_s$. Similarly, for a matrix $\mathbf{A} = (a_{ij}) \in \mathbb{Z}_q^{n\times m}$ we define $[\mathbf{A}]_s$ as the implicit representation of $\mathbf{A}$ in $\mathbb{G}_s$. $\mathsf{Span}(\mathbf{A}) := \{\mathbf{A}\mathbf{r} | \mathbf{r} \in \mathbb{Z}_q^m\} \subset \mathbb{Z}_q^n$ denotes the linear span of $\mathbf{A}$, and similarly $\mathsf{Span}([\mathbf{A}]_s) := \{[\mathbf{A}\mathbf{r}]_s | \mathbf{r} \in \mathbb{Z}_q^m\} \subset \mathbb{G}_s^n$. Note that it is

efficient to compute $[\mathbf{AB}]_s$ given $([\mathbf{A}]_s, \mathbf{B})$ or $(\mathbf{A}, [\mathbf{B}]_s)$ with matching dimensions. We define $[\mathbf{A}]_1 \circ [\mathbf{B}]_2 := e([\mathbf{A}]_1, [\mathbf{B}]_2) = [\mathbf{AB}]_T$, which can be efficiently computed given $[\mathbf{A}]_1$ and $[\mathbf{B}]_2$.

Next we recall the definition of the matrix Diffie-Hellman (MDDH) and related assumptions [13].

Definition 1 (Matrix Distribution). *Let $k, \ell \in \mathbb{N}$ with $\ell > k$. We call $\mathcal{D}_{\ell,k}$ a* matrix distribution *if it outputs matrices in $\mathbb{Z}_q^{\ell \times k}$ of full rank k in polynomial time.*

Without loss of generality, we assume the first k rows of $\mathbf{A} \xleftarrow{\$} \mathcal{D}_{\ell,k}$ form an invertible matrix. The $\mathcal{D}_{\ell,k}$-matrix Diffie-Hellman problem is to distinguish the two distributions $([\mathbf{A}], [\mathbf{Aw}])$ and $([\mathbf{A}], [\mathbf{u}])$ where $\mathbf{A} \xleftarrow{\$} \mathcal{D}_{\ell,k}$, $\mathbf{w} \xleftarrow{\$} \mathbb{Z}_q^k$ and $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^\ell$.

Definition 2 ($\mathcal{D}_{\ell,k}$-matrix Diffie-Hellman Assumption). *Let $\mathcal{D}_{\ell,k}$ be a matrix distribution and $s \in \{1, 2, T\}$. We say that the* $\mathcal{D}_{\ell,k}$-matrix Diffie-Hellman *($\mathcal{D}_{\ell,k}$-MDDH)* assumption *holds relative to* PGGen *in group $\mathbb{G}_s$ if for all PPT adversaries $\mathcal{A}$, it holds that*

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

is negligible where the probability is taken over $\mathcal{PG} \xleftarrow{\$} \mathsf{PGGen}(1^\lambda)$, $\mathbf{A} \xleftarrow{\$} \mathcal{D}_{\ell,k}$, $\mathbf{w} \xleftarrow{\$} \mathbb{Z}_q^k$ and $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^\ell$.

The uniform distribution is a particular matrix distribution that deserves special attention, as an adversary breaking the $\mathcal{U}_{\ell,k}$ assumption can also distinguish between real MDDH tuples and random tuples for all other possible matrix distributions. For uniform distributions, they stated in [14] that $\mathcal{U}_k$-MDDH and $\mathcal{U}_{\ell,k}$-MDDH assumptions are equivalent.

Definition 3 (Uniform Distribution). *Let $k, \ell \in \mathbb{N}_+$ with $\ell > k$. We call $\mathcal{U}_{\ell,k}$ a* uniform distribution *if it outputs uniformly random matrices in $\mathbb{Z}_q^{\ell \times k}$ of rank k in polynomial time. Let $\mathcal{U}_k := \mathcal{U}_{k+1,k}$.*

Lemma 1 ($\mathcal{U}_{\ell,k}$-MDDH $\Leftrightarrow$ $\mathcal{U}_k$-MDDH [14]). *Let $\ell, k \in \mathbb{N}_+$ with $\ell > k$. An $\mathcal{U}_{\ell,k}$-MDDH instance is as hard as an $\mathcal{U}_k$-MDDH instance. More precisely, for each adversary $\mathcal{A}$ there exists an adversary $\mathcal{B}$ and vice versa with*

$$\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_{\ell,k},\mathsf{PGGen},s}(\mathcal{A}) = \mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},s}(\mathcal{B})$$

and $T(\mathcal{A}) \approx T(\mathcal{B})$.

Proof. An $\mathcal{U}_{\ell,k}$-MDDH instance $(\mathcal{PG}, [\mathbf{A}]_s, [\mathbf{v}]_s)$ can be transformed into an $\mathcal{U}_k$-MDDH by picking uniformly random a full-rank matrix $\mathbf{T} \in \mathbb{Z}_q^{(k+1)\times \ell}$ and returning $(\mathcal{PG}, [\mathbf{TA}]_s, [\mathbf{Tv}]_s)$.

For the other direction one picks uniformly random a full-rank matrix $\mathbf{T}' \in \mathbb{Z}_q^{\ell \times (k+1)}$ to turn the $\mathcal{U}_k$-MDDH instance $(\mathcal{PG}, [\mathbf{A}]_s, [\mathbf{v}]_s)$ into an $\mathcal{U}_{\ell,k}$-MDDH instance $(\mathcal{PG}, [\mathbf{T}'\mathbf{A}]_s, [\mathbf{T}'\mathbf{v}]_s)$. □

Lemma 2 ($\mathcal{D}_{\ell,k}$-MDDH $\Rightarrow \mathcal{U}_k$-MDDH [13]). *Let $\ell, k \in \mathbb{N}_+$ with $\ell > k$ and let $\mathcal{D}_{\ell,k}$ be a matrix distribution. A $\mathcal{U}_k$-MDDH instance is at least as hard as an $\mathcal{D}_{\ell,k}$ instance. More precisely, for each adversary $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},s}(\mathcal{A}) \leq \mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{D}_{\ell,k},\mathsf{PGGen},s}(\mathcal{B})$$

and $T(\mathcal{A}) \approx T(\mathcal{B})$.

For $Q \in \mathbb{N}_+$, $\mathbf{W} \xleftarrow{\$} \mathbb{Z}_q^{k\times Q}, \mathbf{U} \xleftarrow{\$} \mathbb{Z}_q^{\ell\times Q}$, consider the Q-fold $\mathcal{D}_{\ell,k}$-MDDH problem which is distinguishing the distributions $(\mathcal{PG}, [\mathbf{A}], [\mathbf{AW}])$ and $(\mathcal{PG}, [\mathbf{A}], [\mathbf{U}])$. That is, the Q-fold $\mathcal{D}_{\ell,k}$-MDDH problem contains Q independent instances of the $\mathcal{D}_{\ell,k}$-MDDH problem (with the same $\mathbf{A}$ but different $\mathbf{w}_i$). By a hybrid argument, one can show that the two problems are equivalent, where the reduction loses a factor Q. The following lemma gives a tight reduction.

Lemma 3 (Random Self-reducibility [13]). *For $\ell > k$ and any matrix distribution $\mathcal{D}_{\ell,k}$, the $\mathcal{D}_{\ell,k}$-MDDH assumption is random self-reducible. In particular, for any $Q \in \mathbb{N}_+$ and any adversary $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$(\ell-k)\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{D}_{\ell,k},\mathsf{PGGen},s}(\mathcal{A}) + \frac{1}{q-1} \geq \mathsf{Adv}^{Q\text{-}\mathsf{mddh}}_{\mathcal{D}_{\ell,k},\mathsf{PGGen},s}(\mathcal{B}) := \\ \left|\Pr[\mathcal{B}(\mathcal{PG}, [\mathbf{A}], [\mathbf{AW}] \Rightarrow 1)] - \Pr[\mathcal{B}(\mathcal{PG}, [\mathbf{A}], [\mathbf{U}] \Rightarrow 1)]\right|,$$

where $\mathcal{PG} \xleftarrow{\$} \mathsf{PGGen}(1^\lambda)$, $\mathbf{A} \xleftarrow{\$} \mathcal{D}_{\ell,k}$, $\mathbf{W} \xleftarrow{\$} \mathbb{Z}_q^{k\times Q}$, $\mathbf{U} \xleftarrow{\$} \mathbb{Z}_q^{(k+1)\times Q}$, and $T(\mathcal{B}) \approx T(\mathcal{A}) + Q \cdot \mathsf{poly}(\lambda)$, where poly is a polynomial independent of $\mathcal{A}$.

To reduce the Q-fold $\mathcal{U}_{\ell,k}$-MDDH assumption to the $\mathcal{U}_k$-MDDH assumption we have to apply Lemma 3 to get from Q-fold $\mathcal{U}_{\ell,k}$-MDDH to standard $\mathcal{U}_{\ell,k}$-MDDH and then Lemma 1 to get from $\mathcal{U}_{\ell,k}$-MDDH to $\mathcal{U}_k$-MDDH. Thus for every adversary $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with

$$\mathsf{Adv}^{Q\text{-}\mathsf{mddh}}_{\mathcal{U}_{\ell,k},\mathsf{PGGen},s}(\mathcal{A}) \leq (\ell-k)\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},s}(\mathcal{B}) + \frac{1}{q-1}.$$

The following Lemma is often helpful with the uniform matrix distribution.

Lemma 4.

$$\Pr\left[\mathrm{rank}(\mathbf{A}) = k \mid \mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{k\times k}\right] \geq 1 - \frac{1}{q-1}$$

A proof can be found in Appendix A.

2.2 Pseudorandom Functions

For the IBE construction we need pseudorandom functions (PRFs).

Definition 4 (Pseudorandom Function). *A* family of pseudorandom functions *is a tuple $\mathcal{F} := (\mathsf{Gen}_{\mathsf{PRF}}, \mathsf{PRF})$ of polynomial-time algorithms with:*

- $\mathcal{K} \xleftarrow{\$} \mathsf{Gen}_{\mathsf{PRF}}(1^\lambda)$ *is a probabilistic algorithm that gets the security parameter* 1^λ *and returns a (private) key* $\mathcal{K}$.
- PRF *is a deterministic algorithm that gets a key* $\mathcal{K}$ *and an input* $X \in \mathcal{D}$ *and outputs* $\mathsf{PRF}_{\mathcal{K}}(X) \in \mathcal{R}$, *where* $\mathcal{D}$ *is the domain set and* $\mathcal{R}$ *is the finite range set.*

The security notion for pseudorandom functions is pseudorandomness.

Definition 5 (Pseudorandomness). *A family of pseudorandom functions* $\mathcal{F} := (\mathsf{Gen}_{\mathsf{PRF}}, \mathsf{PRF})$ *is* pseudorandom *if for all PPT adversaries* $\mathcal{A}$,

$$\mathsf{Adv}^{\mathsf{pr}}_{\mathcal{F}}(\mathcal{A}) := \left|\Pr\left[\mathcal{A}^{\mathsf{PRF}_{\mathcal{K}}(\cdot)} \Rightarrow 1 \mid \mathcal{K} \xleftarrow{\$} \mathsf{Gen}_{\mathsf{PRF}}(1^\lambda)\right] - \Pr\left[\mathcal{A}^{\mathsf{RF}(\cdot)} \Rightarrow 1\right]\right|$$

is negligible in λ. *The notion* $\mathcal{A}^{f(\cdot)}$ *means* $\mathcal{A}$ *has oracle access to the function* f *and* $\mathsf{RF} : \mathcal{D} \to \mathcal{R}$ *is random function (i.e. a function that maps every input to a uniform random value from* $\mathcal{R}$*).*

2.3 Affine MACs

The HIBEs in this paper are constructed in the BKP framework: The HIBEs are obtained from a Message Authentication Code with suitable algebraic structures (affine MAC with levels). The main work is to achieve tight security in the multi-challenge setting for the MACs.

To achieve this, we need to generalize the structure of the affine MAC with levels slightly and allow that $\mathbf{X}$ can be a matrix (instead of a vector) and $\mathbf{x}'$ can be a vector (instead of only a scalar value). Please note that in the definition in this paper, $\mathbf{X}$ is transposed compared to the original affine MAC with levels definition.

Definition 6 (Affine MAC with Levels). *An* affine MAC with levels MAC *consists of three PPT algorithms* $(\mathsf{Gen}_{\mathsf{MAC}}, \mathsf{Tag}, \mathsf{Ver}_{\mathsf{MAC}})$ *with the following properties:*

- $\mathsf{Gen}_{\mathsf{MAC}}(\mathbb{G}_2, q, P_2)$ *gets a description of a prime-order group* $(\mathbb{G}_2, q, P_2)$ *and returns a secret key* $\mathsf{sk}_{\mathsf{MAC}} := \left(\mathbf{B}, (\mathbf{X}_{l,i,j})_{1\le l\le \ell(p), 1\le i\le L, 1\le j\le \ell'(l,i)}, \mathbf{x}'\right)$ *where* $\mathbf{B} \in \mathbb{Z}_q^{n\times n'}$, $\mathbf{X}_{l,i,j} \in \mathbb{Z}_q^{\eta\times n}$ *for* $l \in \{1,\dots,\ell(L)\}$, $i \in \{1,\dots,L\}$, *and* $j \in \{0,\dots,\ell'(l,i)\}$ *and* $\mathbf{x}' \in \mathbb{Z}_q^{\eta}$.
- $\mathsf{Tag}\left(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m} \in \mathcal{S}^{p\le L}\right)$ *returns a tag* $\tau := \left(([\mathbf{t}_l]_2)_{1\le l\le \ell(p)}, [\mathbf{u}]_2\right)$ *where*

$$\begin{aligned} \mathbf{t}_l &:= \mathbf{B}\mathbf{s}_l \quad \text{for } \mathbf{s}_l \xleftarrow{\$} \mathbb{Z}_q^{n'} \quad (1 \le l \le \ell(p)) \\ \mathbf{u} &:= \sum_{l=1}^{\ell(p)} \left(\sum_{i=1}^{p} \sum_{j=1}^{\ell'(l,i)} f_{l,i,j}(\mathsf{m}_{|i}) \mathbf{X}_{l,i,j} \right) \mathbf{t}_l + \mathbf{x}' \,. \end{aligned} \tag{5}$$

- $\mathsf{Ver}_{\mathsf{MAC}}\left(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m}, \tau = \left(([\mathbf{t}_l]_2)_{1\le l\le \ell(p)}, [\mathbf{u}]_2\right)\right)$ *checks, whether Equation (5) holds.*

$\underline{\text{INIT}_{\mathsf{MAC}}}$: $\mathcal{PG} \xleftarrow{\$} \mathsf{PGGen}(1^\lambda)$ **parse** $\mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$ $\mathsf{sk}_{\mathsf{MAC}} \xleftarrow{\$} \mathsf{Gen}_{\mathsf{MAC}}(\mathbb{G}_2, q, P_2)$ **parse** $\mathsf{sk}_{\mathsf{MAC}} =: \left(\mathbf{B}, (\mathbf{X}_j)_{1 \le j \le \ell}, \mathbf{x}'\right)$ **return** $\mathcal{PG}$ $\underline{\text{EVAL}(\mathsf{m} \in \mathcal{S})}$: $\mathcal{Q}_{\mathcal{M}} := \mathcal{Q}_{\mathcal{M}} \cup \{\mathsf{m}\}$ **return** $\mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m})$ $\underline{\text{FINALIZE}_{\mathsf{MAC}}(\beta \in \{0,1\})}$: **return** $(\mathcal{C}_{\mathcal{M}} \cap \mathcal{Q}_{\mathcal{M}} = \emptyset) \wedge \beta$	$\underline{\text{CHAL}(\mathsf{m}^\star \in \mathcal{S})}$: $\mathcal{C}_{\mathcal{M}} := \mathcal{C}_{\mathcal{M}} \cup \{\mathsf{m}^\star\}$ $\mathbf{h} \xleftarrow{\$} \mathbb{Z}_q^\eta$ $\mathbf{h}_0 := \left(\sum_{j=1}^{\ell} f_j(\mathsf{m}^\star)\mathbf{X}_j^\top\right)\mathbf{h}$ $\boxed{\mathbf{h}_0 \xleftarrow{\$} \mathbb{Z}_q^n}$ $h_1 = (\mathbf{x}')^\top \mathbf{h} \in \mathbb{Z}_q$ $\boxed{h_1 \xleftarrow{\$} \mathbb{Z}_q}$ **return** $\left([\mathbf{h}]_1, [\mathbf{h}_0]_1, [h_1]_T\right)$

Fig. 2. Games $\mathsf{mPR\text{-}CMA}_{\mathsf{real}}$ and $\boxed{\mathsf{mPR\text{-}CMA}_{\mathsf{rand}}}$ for defining mPR-CMA security for affine MACs.

The messages of MAC *have the form* $\mathsf{m} = (\mathsf{m}_1, \ldots, \mathsf{m}_p)$ *where* $p \le L$ *and* $\mathsf{m}_i \in \mathcal{S}$. *After the transformation to an HIBE,* $\mathcal{S}$ *will be the base set of the identity space and* L *will be the maximum number of levels. The functions* $f_{l,i,j} : \mathcal{S}^i \to \mathbb{Z}_q$ *must be public, efficiently computable functions. The parameters* $\ell : \{1, \ldots, p\} \to \mathbb{N}_+$, $n, n', \eta \in \mathbb{N}_+$ *and* $\ell' : \{1, \ldots, p\} \times \{1, \ldots, L\} \to \mathbb{N}_+$ $(1 \le i \le L)$ *are arbitrary, scheme-depending parameters. The function* ℓ *must be monotonous increasing.*

A delegatable affine MAC is an affine MAC with levels with $\ell(p) = 1$ and an affine MAC is a delegatable affine MAC with $L = 1$. We can use affine MACs with levels to build HIBEs, delegatable affine MACs to build anonymous HIBEs and affine MACs to build anonymous IBEs.

SECURITY. To build anonymous IBE, we need an affine MAC that satisfies multi-challenge pseudorandomness against chosen message attacks (mPR-CMA) security.

We require multi-challenge hierarchical pseudorandomness against chosen-message attacks (mHPR-CMA) for affine MACs with levels to obtain mIND-HID-CPA and mIND-HID-CCA secure HIBEs.The security notion is defined by the games in Figure 3.

Definition 7 (mXPR-CMA Security). *An affine MAC (with levels)* MAC *is* mXPR-CMA-secure *for* $X \in \{\varepsilon, \mathsf{H}\}$ *in* $\mathbb{G}_2$ *if for all PPT adversaries* $\mathcal{A}$ *the function*

$$\mathsf{Adv}^{m x \mathsf{pr\text{-}cma}}_{\mathsf{MAC},\mathbb{G}_2}(\mathcal{A}) := \left|\Pr\left[\mathsf{mXPR\text{-}CMA}^{\mathcal{A}}_{\mathsf{real}} \Rightarrow 1\right] - \Pr\left[\mathsf{mXPR\text{-}CMA}^{\mathcal{A}}_{\mathsf{rand}} \Rightarrow 1\right]\right|$$

is negligible.

$\underline{\text{INIT}_{\mathsf{MAC}}}$:
$\mathcal{PG} \xleftarrow{\$} \mathsf{PGGen}\left(1^\lambda\right)$
parse $\mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
$\mathsf{sk}_{\mathsf{MAC}} \xleftarrow{\$} \mathsf{Gen}_{\mathsf{MAC}}(\mathbb{G}_2, q, P_2)$
$\mathsf{sk}_{\mathsf{MAC}} =: \left(\mathbf{B}, (\mathbf{X}_{l,i,j})_{\substack{1\le l\le \ell(p), 1\le i\le L, \\ 1\le j\le \ell'(l,i)}}, \mathbf{x}'\right)$
$\mathsf{dk} := \left([\mathbf{X}_{l,i,j}\mathbf{B}]_2\right)_{\substack{1\le l\le \ell(p), 1\le i\le L \\ 1\le j\le \ell'(l,i)}}$
return $\left(\mathcal{PG}, [\mathbf{B}]_2, \mathsf{dk}\right)$

$\underline{\text{EVAL}(\mathsf{m} \in \mathcal{S}^p)}$:
$\mathcal{Q}_{\mathcal{M}} := \mathcal{Q}_{\mathcal{M}} \cup \{\mathsf{m}\}$
$\left(\left([\mathbf{t}_l]_2\right)_{1\le l\le \ell(p)}, [\mathbf{u}]_2\right) \xleftarrow{\$} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m})$
for $l \in \{1, \dots, \ell(p)\}$, $i \in \{p+1, \dots, L\}$, $j \in \{1, \dots, \ell'(l,i)\}$ **do** $\mathbf{d}_{l,i,j} := \mathbf{X}_{l,i,j}\mathbf{t}_l$
$\mathsf{tdk} := \left([\mathbf{d}_{l,i,j}]_2\right)_{1\le l\le \ell(p), p+1\le i\le L, 1\le j\le \ell'(l,i)}$
return $\left(\left([\mathbf{t}_l]_2\right)_{1\le l\le \ell(p)}, [\mathbf{u}]_2, \mathsf{tdk}\right)$

$\underline{\text{CHAL}(\mathsf{m}^\star \in \mathcal{S}^p)}$:
$\mathcal{C}_{\mathcal{M}} := \mathcal{C}_{\mathcal{M}} \cup \{\mathsf{m}^\star\}$
$\mathbf{h} \xleftarrow{\$} \mathbb{Z}_q^\eta$
for $l \in \{1, \dots, \ell(p)\}$ **do**
$\quad \mathbf{h}_{0,l} := \left(\sum_{i=1}^{L} \sum_{j=1}^{\ell'(l,i)} f_{l,i,j}\left(\mathsf{m}^\star_{|i}\right)\mathbf{X}_{l,i,j}^\top\right)\mathbf{h}$
$h_1 = (\mathbf{x}')^\top \mathbf{h} \in \mathbb{Z}_q$
$\boxed{h_1 \xleftarrow{\$} \mathbb{Z}_q}$
return $\left([\mathbf{h}]_1, \left([\mathbf{h}_{0,l}]_1\right)_{1\le l\le \ell(p)}, [h_1]_T\right)$

$\underline{\text{FINALIZE}_{\mathsf{MAC}}(\beta \in \{0,1\})}$:
return $\left(\bigcup_{\mathsf{m}^\star \in \mathcal{C}_{\mathcal{M}}} \mathsf{Prefix}(\mathsf{m}^\star) \cap \mathcal{Q}_{\mathcal{M}} = \emptyset\right) \wedge \beta$

Fig. 3. Games $\mathsf{mHPR\text{-}CMA}_{\mathsf{real}}$ and $\boxed{\mathsf{mHPR\text{-}CMA}_{\mathsf{rand}}}$ for defining mHPR-CMA security for affine MACs with levels.

3 Delegatable Affine MACs with Tight Multi-Challenge Security.

3.1 Warm-up: IBE

First, we present the technique to handle multiple challenge queries in the IBE setting ($L = 1$). The MAC is given in Figure 4. This affine MAC has identity space $\mathcal{S} = \{0,1\}^\alpha$ (for arbitrary $\alpha \in \mathbb{N}_+$) and uses $n = 2k$, $n' = k$, $\eta = k$ and $\ell' = \alpha$. To match the formal definition, $\mathbf{X}_{j,b}$ should be renamed to $\mathbf{X}_{2j-b}$ and $f_{2j-b}(\mathsf{m}) := \left(\mathsf{m}_j \stackrel{?}{=} b\right)$. The MAC looks very similar to the one in [25] and achieves the same security and very similar efficiency, however the security proof is quite different. A comparison of the resulting IBE with other tightly secure IBEs can be found in Table 2.

As in [25], we need to ensure that the adversary can only query one tag per message. The key generator can ensure this by making the tags deterministic. He can achieve this by storing the generated tags for duplicated queries (stateful scheme) or by generating the randomness with a pseudorandom function. We have done the later in our presentation. The affine MACs with levels we present later solve this by having rerandomizable tags. Of course, they can be used as affine MAC as well by setting $L = 1$, but this comes at the cost of being slightly less efficient.

Scheme	A	$\lvert\mathsf{mpk}\rvert$	$\lvert\mathsf{usk}\rvert$	$\lvert\mathsf{C}\rvert$	Loss	MC	Ass.
CW13 [10]	✗	$2k^2(2n+1)\lvert\mathbb{G}_1\rvert + k\lvert\mathbb{G}_T\rvert$	$4k\lvert\mathbb{G}_2$	$4k\lvert\mathbb{G}_1$	$\mathbf{O}(n)$	✗	k-LIN
BKP14 [5]	✓	$(2nk^2+2k)\mathbb{G}_1\rvert$	$(2k+1)\lvert\mathbb{G}_2\rvert$	$(2k+1)\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(\lambda)$	✗	k-LIN
AHY15 [3]	✓	$(16n+8)\lvert\mathbb{G}_1\rvert + 2\lvert\mathbb{G}_T\rvert$	$8\lvert\mathbb{G}_2\rvert$	$8\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(n)$	✓	DLIN
GCD$^+$16$_1$ [20]	✗	$(6nk^2+3k^2)\lvert\mathbb{G}_1\rvert + k\lvert\mathbb{G}_T\rvert$	$6k\lvert\mathbb{G}_2\rvert$	$6k\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(n)$	✓	k-LIN
GCD$^+$16$_2$ [20]	✗	$(4nk^2+2k^2)\lvert\mathbb{G}_1\rvert + k\lvert\mathbb{G}_T\rvert$	$4k\lvert\mathbb{G}_2\rvert$	$4k\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(n)$	✓	k-LINAI
GDCC16 [21]	✓	$(2nk^2+3k^2)\lvert\mathbb{G}_1\rvert + k\lvert\mathbb{G}_T\rvert$	$4k\lvert\mathbb{G}_2\rvert$	$4k\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(n)$	✓	k-LIN
HJP18 [25]	✓	$((3+n)k^2+k)\lvert\mathbb{G}_1\rvert$	$4k\lvert\mathbb{G}_2\rvert$	$4k\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(n)$	✓	k-LIN
Ours	✓	$((2+2n)k^2+k)\lvert\mathbb{G}_1\rvert$	$4k\lvert\mathbb{G}_2\rvert$	$4k\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(n)$	✓	k-LIN

Table 2. Comparison of IBEs in prime-order pairing groups with tight adaptive IND-ID-CPA-security in the standard model based on static assumptions. The schemes in the last two rows can also be made IND-ID-CCA secure. The second column indicates whether an IBE is anonymous (✓) or not (✗). The identity space is $\{0,1\}^n$. '$\lvert\mathsf{mpk}\rvert$,' '$\lvert\mathsf{usk}\rvert$,' and '$\lvert\mathsf{C}\rvert$' stand for the size of the master public key, the user secret key and a ciphertext, respectively. We count the number of group elements in $\mathbb{G}_1, \mathbb{G}_2$, and $\mathbb{G}_T$. For a scheme that works in symmetric pairing groups, we write $\mathbb{G}(:= \mathbb{G}_1 = \mathbb{G}_2)$. The last but one column indicates whether the adversary is allowed to query multiple challenge ciphertexts (✓) or just one (✗). The last column shows the underlying security assumption.

$\underline{\mathsf{Gen}_{\mathsf{MAC}}(\mathbb{G}_2, q, P_2)}$:
$\mathcal{K} \xleftarrow{\$} \mathsf{Gen}_{\mathsf{PRF}}\big(1^\lambda\big)$
for $j \in \{1,\dots,\alpha\},\ b \in \{0,1\}$ **do** $\mathbf{X}_{j,b} \xleftarrow{\$} \mathbb{Z}_q^{k\times 2k}$
$\mathbf{x}' \xleftarrow{\$} \mathbb{Z}_q^k$
return $\mathsf{sk}_{\mathsf{MAC}} := \big(\mathcal{K}, (\mathbf{X}_{j,b})_{1\le j\le\alpha, b\in\{0,1\}}, \mathbf{x}'\big)$

$\underline{\mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m} \in \mathcal{S})}$:
parse $\mathsf{sk}_{\mathsf{MAC}} =: \big(\mathcal{K}, (\mathbf{X}_{j,b})_{1\le j\le\alpha, b\in\{0,1\}}, \mathbf{x}'\big)$
$\mathbf{t} := \mathsf{PRF}_{\mathcal{K}}(\mathsf{m}) \in \mathbb{Z}_q^{2k}$
$\mathbf{u} := \sum_{j=1}^{\alpha} \mathbf{X}_{j,\mathsf{m}_j}\mathbf{t} + \mathbf{x}'$
return $\big([\mathbf{t}]_2, [\mathbf{u}]_2\big)$

$\underline{\mathsf{Ver}_{\mathsf{MAC}}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m} \in \mathcal{S}, \tau)}$:
parse $\mathsf{sk}_{\mathsf{MAC}} =: \big(\mathcal{K}, (\mathbf{X}_{j,b})_{1\le j\le\alpha, b\in\{0,1\}}, \mathbf{x}'\big)$
parse $\tau =: \big([\mathbf{t}]_2, [\mathbf{u}]_2\big)$
return $\mathbf{u} \stackrel{?}{=} \sum_{j=1}^{\alpha} \mathbf{X}_{j,\mathsf{m}_j}\mathbf{t} + \mathbf{x}'$

Fig. 4. The new multi-challenge tightly secure affine MAC MAC_{mc}.

Theorem 1 (Security of MAC_{mc}). *MAC_{mc} is tightly* mPR-CMA *secure in $\mathbb{G}_2$ under the $\mathcal{U}_k$-*MDDH *assumption for $\mathbb{G}_1$, the $\mathcal{U}_k$-*MDDH *assumption for $\mathbb{G}_2$ and the pseudorandomness of $\mathcal{F} := (\mathsf{Gen}_{\mathsf{PRF}}, \mathsf{PRF})$. More precisely, for all adversaries $\mathcal{A}$ there exists adversaries $\mathcal{B}_1$, $\mathcal{B}_2$ and $\mathcal{B}_3$ with*

$$\mathsf{Adv}^{\mathsf{mpr\text{-}cma}}_{\mathsf{MAC}_{mc}}(\mathcal{A}) \leq 8k\alpha\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},2}(\mathcal{B}_1) + (k\alpha + 2k + 1)\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}_2) + 2\mathsf{Adv}^{\mathsf{pr}}_{\mathcal{F}}(\mathcal{B}_3) + \frac{(Q_c+10)\alpha+4}{q-1} + \frac{2Q_e}{q^{2k}}$$

and $T(\mathcal{B}_1) \approx T(\mathcal{B}_2) \approx T(\mathcal{B}_3) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$, where Q_e resp. Q_c denotes the number of Eval *resp.* Chal *queries of $\mathcal{A}$ and* poly *is a polynomial independent of $\mathcal{A}$.*

Proof. The proof uses a hybrid argument with the hybrids G_0, G_1, $\mathsf{G}_{2,\hat{\jmath},0}$ for $\hat{\jmath} \in \{0,\dots,\alpha\}$, $\mathsf{G}_{2,\hat{\jmath},1}$–$\mathsf{G}_{2,\hat{\jmath},3}$ for $\hat{\jmath} \in \{0,\dots,\alpha-1\}$ and finally G_3–G_5. They are given in Table 3. They make use of the random functions $\mathsf{RF} : \mathcal{S} \to \mathbb{Z}_q^{2k}$, $\mathsf{RF}' : \mathcal{S} \to \mathbb{Z}_q^{k}$, $\mathsf{RF}_{\hat{\jmath}} : \{0,1\}^{\hat{\jmath}} \to \mathbb{Z}_q^{k\times 2k}$, $\mathsf{ZF}_{\hat{\jmath}} : \{0,1\}^{\hat{\jmath}} \to \mathbb{Z}_q^{k\times k}$ and $\mathsf{OF}_{\hat{\jmath}} : \{0,1\}^{\hat{\jmath}} \to \mathbb{Z}_q^{k\times k}$ for $\hat{\jmath} \in \{1,\dots,\alpha\}$ and $\widetilde{\mathsf{RF}} : \mathcal{S} \to \mathbb{Z}_q^{k}$.

Lemma 5 ($\mathsf{G}_0 \rightsquigarrow \mathsf{G}_1$). *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}_0^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_1^{\mathcal{A}} \Rightarrow 1\right]\right| \leq \mathsf{Adv}^{\mathsf{pr}}_{\mathcal{F}}(\mathcal{B})$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. The value $\mathbf{t}$ for in the Eval oracle is chosen randomly in game G_1 instead of pseudorandom in game G_0. This leads to a straightforward reduction to the pseudorandomness of $\mathcal{F} := (\mathsf{Gen}_{\mathsf{PRF}}, \mathsf{PRF})$. □

Lemma 6 ($\mathsf{G}_1 \rightsquigarrow \mathsf{G}_{2,0,0}$).

$$\Pr\left[\mathsf{G}_1^{\mathcal{A}} \Rightarrow 1\right] = \Pr\left[\mathsf{G}_{2,0,0}^{\mathcal{A}} \Rightarrow 1\right]$$

Proof. In game G_1 replace $\mathbf{X}_{1,b}$ with $\mathbf{X}_{1,b} + \mathsf{RF}_0(\varepsilon)$ for $b \in \{0,1\}$ to obtain game $\mathsf{G}_{2,0,0}$. □

Lemma 7 ($\mathsf{G}_{2,\hat{\jmath},0} \rightsquigarrow \mathsf{G}_{2,\hat{\jmath},1}$). *For $\hat{\jmath} < \alpha$ and all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}_{2,\hat{\jmath},0}^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_{2,\hat{\jmath},1}^{\mathcal{A}} \Rightarrow 1\right]\right| \leq 2k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},2}(\mathcal{B}) + \frac{2}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

A proof can be found in Appendix A.

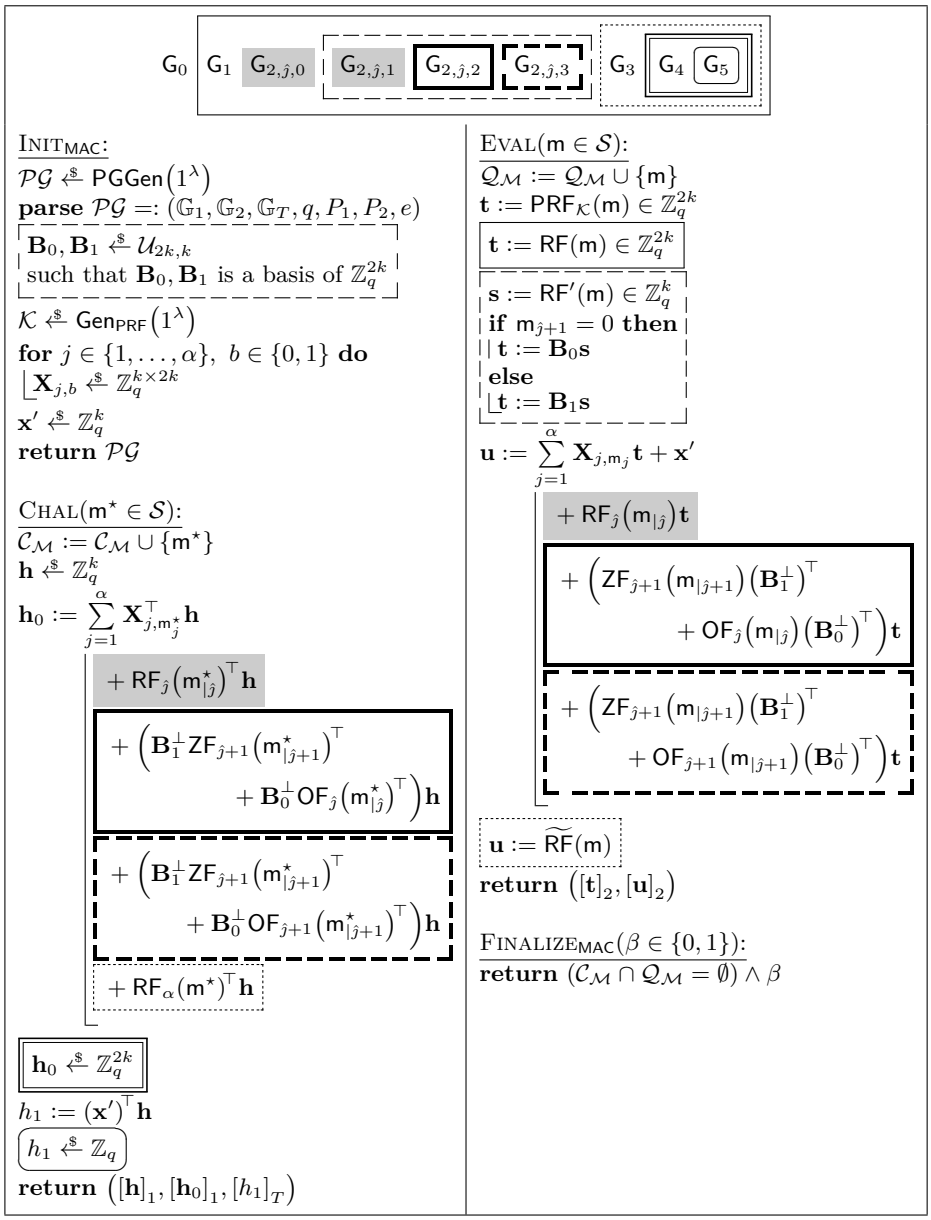


Fig. 5. Hybrids for the security proof of MAC_{mc}.

Hybrid	$\mathbf{t}$ uniform in	$r_{\mathbf{u}}(\mathsf{m})$	$r_{\mathbf{h}_0}(\mathsf{m})$	Transition
G_0	$\mathbb{Z}_q^{2k}$ (pseudorandom)	0		Original game
G_1	$\mathbb{Z}_q^{2k}$	0		PRF
$\mathsf{G}_{2,\hat{\jmath},0}$	$\mathbb{Z}_q^{2k}$	$\mathsf{RF}_{\hat{\jmath}}(\mathsf{m}_{\lvert\hat{\jmath}})$		Identical
$\mathsf{G}_{2,\hat{\jmath},1}$	**if** $\mathsf{m}_{\hat{\jmath}+1}=0$ **then** $\mathsf{Span}(\mathbf{B}_0)$ **else** $\mathsf{Span}(\mathbf{B}_1)$	$\mathsf{RF}_{\hat{\jmath}}(\mathsf{m}_{\lvert\hat{\jmath}})$		$\mathcal{U}_k$-MDDH in $\mathbb{G}_2$
$\mathsf{G}_{2,\hat{\jmath},2}$		$\left(\mathsf{ZF}_{\hat{\jmath}+1}(\mathsf{m}_{\lvert\hat{\jmath}+1})(\mathbf{B}_1^\perp)^\top + \mathsf{OF}_{\hat{\jmath}}(\mathsf{m}_{\lvert\hat{\jmath}})(\mathbf{B}_0^\perp)^\top\right)$		$\mathcal{U}_k$-MDDH in $\mathbb{G}_1$
$\mathsf{G}_{2,\hat{\jmath},3}$		$\left(\mathsf{ZF}_{\hat{\jmath}+1}(\mathsf{m}_{\lvert\hat{\jmath}+1})(\mathbf{B}_1^\perp)^\top + \mathsf{OF}_{\hat{\jmath}+1}(\mathsf{m}_{\lvert\hat{\jmath}+1})(\mathbf{B}_0^\perp)^\top\right)$		$\mathcal{U}_k$-MDDH in $\mathbb{G}_1$
$\mathsf{G}_{2,\hat{\jmath}+1,0}$	$\mathbb{Z}_q^{2k}$	$\mathsf{RF}_{\hat{\jmath}+1}(\mathsf{m}_{\lvert\hat{\jmath}+1})$		$\mathcal{U}_k$-MDDH in $\mathbb{G}_2$
G_3	$\mathbb{Z}_q^{2k}$	uniform random	$\mathsf{RF}_\alpha(\mathsf{m})$	Statistically close
G_4	$\mathbb{Z}_q^{2k}$	uniform random	uniform random	$\mathcal{U}_k$-MDDH in $\mathbb{G}_1$
G_5	$\mathbb{Z}_q^{2k}$	uniform random	uniform random	$\mathcal{U}_k$-MDDH in $\mathbb{G}_1$

Table 3. Summary of the hybrids of Figure 5. Non-duplicated EVAL queries draw (pseudo-)randomly $\mathbf{t}$ from the set described by the second column and add the randomness $r_{\mathbf{u}}(\mathsf{m})\mathbf{t}$ to $\mathbf{u}$ or choose $\mathbf{u}$ uniform random. The CHAL queries add the term $r_{\mathbf{h}_0}(\mathsf{m}^\star)^\top\mathbf{h}$ to $\mathbf{h}_0$ or choose $\mathbf{h}_0$ uniform random. The column "Transition" displays how we can switch to this hybrid from the previous one. The background color indicates repeated transitions.

Lemma 8 ($\mathsf{G}_{2,\hat{\jmath},1} \rightsquigarrow \mathsf{G}_{2,\hat{\jmath},2}$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\jmath},1} \Rightarrow 1\right] - \Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\jmath},2} \Rightarrow 1\right]\right| \leq k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}) + \frac{Q_c+2}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e+Q_c)\cdot\mathsf{poly}(\lambda)$.

Proof. First of all, we replace the term $\mathsf{RF}_{\hat{\jmath}}(\mathsf{m}_{\lvert\hat{\jmath}})$ in $\mathsf{G}_{2,\hat{\jmath},1}$ with $\mathsf{ZF}_{\hat{\jmath}}(\mathsf{m}_{\lvert\hat{\jmath}})(\mathbf{B}_1^\perp)^\top + \mathsf{OF}_{\hat{\jmath}}(\mathsf{m}_{\lvert\hat{\jmath}})(\mathbf{B}_0^\perp)^\top$. This does not change the distribution, since $\mathbf{B}_1^\perp, \mathbf{B}_0^\perp$ is a basis of $\mathbb{Z}_q^{2k}$. To show this, we assume $(\mathbf{B}_1^\perp|\mathbf{B}_0^\perp)$ does not have full rank. Since both $\mathbf{B}_1^\perp$ and $\mathbf{B}_0^\perp$ have rank k, there is a non-zero vector $\mathbf{v} \in \mathsf{Span}(\mathbf{B}_1^\perp) \cap \mathsf{Span}(\mathbf{B}_0^\perp)$ such that $(\mathbf{B}_0|\mathbf{B}_1)\mathbf{v} = 0$, which contradicts the fact that $\mathbf{B}_0, \mathbf{B}_1$ is a basis of $\mathbb{Z}_q^{2k}$.

Define

$$\mathsf{ZF}_{\hat{\jmath}+1}(\mathsf{m}_{\lvert\hat{\jmath}+1}) := \begin{cases} \mathsf{ZF}_{\hat{\jmath}}(\mathsf{m}_{\lvert\hat{\jmath}}) & \text{if } \mathsf{m}_{\hat{\jmath}+1}=0 \\ \mathsf{ZF}_{\hat{\jmath}}(\mathsf{m}_{\lvert\hat{\jmath}}) + \mathsf{ZF}'_{\hat{\jmath}}(\mathsf{m}_{\lvert\hat{\jmath}}) & \text{if } \mathsf{m}_{\hat{\jmath}+1}=1 \end{cases},$$

where $\mathsf{ZF}'_{\hat{\jmath}} : \{0,1\}^{\hat{\jmath}} \to \mathbb{Z}_q^{1\times k}$ is another independent random function. Since $\mathsf{ZF}_{\hat{\jmath}}$ does not appear in game $\mathsf{G}_{2,\hat{\jmath},2}$ anymore, $\mathsf{ZF}_{\hat{\jmath}+1}$ is a random function.

Let $\left([\mathbf{D}]_1, [\mathbf{f}_1]_1, \ldots, [\mathbf{f}_{kQ_c}]_1\right)$ be a (kQ_c)-fold $\mathcal{U}_{2k,k}$-MDDH challenge and define $\mathbf{F}_c := \left(\mathbf{f}_{(c-1)k+1} | \ldots | \mathbf{f}_{ck}\right)$ to get Q_c $2k \times k$ matrices, whose column vectors are uniformly random chosen from either $\mathsf{Span}(\mathbf{D})$ or $\mathbb{Z}_q^{2k}$. Then the reduction in Figure 6 can be used to bound the difference between $\mathsf{G}_{2,\hat{\jmath},1}$ and $\mathsf{G}_{2,\hat{\jmath},2}$.

$\underline{\textsc{Init}_{\mathsf{MAC}}}$:
parse $\mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
$\mathbf{B}_0, \mathbf{B}_1 \xleftarrow{\$} \mathcal{U}_{2k,k}$
such that $\mathbf{B}_0, \mathbf{B}_1$ is a basis of $\mathbb{Z}_q^{2k}$
for $j \in \{1, \ldots, \alpha\},\ b \in \{0,1\}$ **do**
$\quad \mathbf{J}_{j,b} \xleftarrow{\$} \mathbb{Z}_q^{k \times 2k}$
$\quad$ **if** $(j,b) \neq (\hat{\jmath}+1, 1)$ **then** $\mathbf{X}_{j,b} := \mathbf{J}_{j,b}$
// Implicit: $\mathbf{X}_{\hat{\jmath}+1,1} := \mathbf{J}_{\hat{\jmath}+1,1} + \left(\mathbf{B}_1^{\perp} \underline{\mathbf{D}} \overline{\mathbf{D}}^{-1}\right)^{\top}$
$\mathbf{x}' \xleftarrow{\$} \mathbb{Z}_q^k$
return $\mathcal{PG}$
 	
$\underline{\textsc{Eval}(\mathsf{m} \in \mathcal{S})}$:
$\mathcal{Q}_{\mathcal{M}} := \mathcal{Q}_{\mathcal{M}} \cup \{\mathsf{m}\}$
$\mathbf{s} := \mathsf{RF}'(\mathsf{m}) \in \mathbb{Z}_q^k$
if $\mathsf{m}_{\hat{\jmath}+1} = 0$ **then**
$\quad \mathbf{t} := \mathbf{B}_0 \mathbf{s}$
else
$\quad \mathbf{t} := \mathbf{B}_1 \mathbf{s}$
$\mathbf{u} := \left(\sum_{j=1}^{\alpha} \mathbf{J}_{j,\mathsf{m}_j} + \mathsf{ZF}_{\hat{\jmath}}\left(\mathsf{m}_{\lvert\hat{\jmath}}\right)\left(\mathbf{B}_1^{\perp}\right)^{\top} + \mathsf{OF}_{\hat{\jmath}}\left(\mathsf{m}_{\lvert\hat{\jmath}}\right)\left(\mathbf{B}_0^{\perp}\right)^{\top} \right) \mathbf{t} + \mathbf{x}'$
return $\left([\mathbf{t}]_2, [\mathbf{u}]_2\right)$
	$\underline{\textsc{Chal}(\mathsf{m}^\star \in \mathcal{S})}$:
	$\mathcal{C}_{\mathcal{M}} := \mathcal{C}_{\mathcal{M}} \cup \{\mathsf{m}^\star\}$
	Let c be the index of the first Chal query on a message with prefix $\mathsf{m}^\star_{\lvert\hat{\jmath}}$.
	$\mathbf{h}' \xleftarrow{\$} \mathbb{Z}_q^k$
	$\mathbf{h} := \overline{\mathbf{F}_c} \mathbf{h}'$
	$\mathbf{h}_0 := \left(\sum_{j=1}^{\alpha} \mathbf{J}_{j,\mathsf{m}^\star_j}^{\top} + \mathbf{B}_1^{\perp} \mathsf{ZF}_{\hat{\jmath}}\left(\mathsf{m}^\star_{\lvert\hat{\jmath}}\right)^{\top} + \mathbf{B}_0^{\perp} \mathsf{OF}_{\hat{\jmath}}\left(\mathsf{m}^\star_{\lvert\hat{\jmath}}\right)^{\top} \right) \mathbf{h}$
	if $\mathsf{m}^\star_{\hat{\jmath}+1} = 1$ **then** $\mathbf{h}_0 := \mathbf{h}_0 + \mathbf{B}_1^{\perp} \underline{\mathbf{F}_c} \mathbf{h}'$
	$h_1 := (\mathbf{x}')^{\top} \mathbf{h}$
	return $\left([\mathbf{h}]_1, [\mathbf{h}_0]_1, [h_1]_T\right)$
	
	$\underline{\textsc{Finalize}_{\mathsf{MAC}}(\beta \in \{0,1\})}$:
	return $(\mathcal{C}_{\mathcal{M}} \cap \mathcal{Q}_{\mathcal{M}} = \emptyset) \wedge \beta$

Fig. 6. Reduction for the transition from $\mathsf{G}_{2,\hat{\jmath},1}$ to $\mathsf{G}_{2,\hat{\jmath},2}$ to the kQ_c-fold $\mathcal{U}_{2k,k}$-MDDH challenge $\left([\mathbf{D}]_1, [\mathbf{F}_1]_1, \ldots, [\mathbf{F}_{Q_c}]_1\right)$.

Eval queries are distributed identically in game $\mathsf{G}_{2,\hat{\jmath},1}$ and $\mathsf{G}_{2,\hat{\jmath},2}$: If $\mathsf{m}_{\hat{\jmath}+1} = 0$, they are the same by the definition of $\mathsf{ZF}_{\hat{\jmath}+1}$. If $\mathsf{m}_{\hat{\jmath}+1} = 1$, $\mathbf{t} \in \mathsf{Span}(\mathbf{B}_0)$ and thus the term $\mathsf{ZF}_{\hat{\jmath}}\left(\mathsf{m}_{\lvert\hat{\jmath}}\right)\left(\mathbf{B}_1^{\perp}\right)^{\top}$ resp. $\mathsf{ZF}_{\hat{\jmath}+1}\left(\mathsf{m}_{\lvert\hat{\jmath}+1}\right)\left(\mathbf{B}_1^{\perp}\right)^{\top}$ cancels out in this query. Note that $\mathsf{ZF}'_{\hat{\jmath}}$ is not evaluated in Eval queries.

Assume that $\overline{\mathbf{D}}$ is invertible. This happens with probability at least $(1 - 1/(q-1))$. For Chal queries we write $\mathbf{F}_c =: \left(\begin{smallmatrix} \overline{\mathbf{D}}\mathbf{W}_c \\ \underline{\mathbf{D}}\mathbf{W}_c + \mathbf{R}_c \end{smallmatrix}\right)$ where $\mathbf{W}_c$ is uniform random in $\mathbb{Z}_q^{k \times k}$ and $\mathbf{R}_c$ is $\mathbf{0} \in \mathbb{Z}_q^{k \times k}$ or uniform random in $\mathbb{Z}_q^{k \times k}$. In the following we will assume that $\mathbf{W}_c$ has full rank. This happens with probability at least $(1 - 1/(q-1))$.

The value $\mathbf{h}$ is uniform random in $\mathbb{Z}_q^k$, since $\mathbf{h}'$ is uniformly random and $\overline{\mathbf{F}_c}$ is an invertible $k \times k$ matrix, since $\overline{\mathbf{D}}$ and $\mathbf{W}_c$ are invertible.

If $\mathsf{m}^\star_{\hat{\jmath}+1} = 0$ the CHAL queries are distributed identically in $\mathsf{G}_{2,\hat{\jmath},1}$ and $\mathsf{G}_{2,\hat{\jmath},2}$. If $\mathsf{m}^\star_{\hat{\jmath}+1} = 1$ The reduction computes $\mathbf{h}_0$ as

$$\begin{aligned}
\mathbf{h}_0 &:= \left(\sum_{j=1}^{\alpha} \mathbf{J}_{j,\mathsf{m}^\star_j}^\top + \mathsf{F}\left(\mathsf{m}^\star_{|\hat{\jmath}}\right)\right)\mathbf{h} + \mathbf{B}_1^\perp \underline{\mathbf{F}_c}\mathbf{h}' \\
&= \left(\sum_{j=1}^{\alpha} \mathbf{J}_{j,\mathsf{m}^\star_j}^\top + \mathsf{F}\left(\mathsf{m}^\star_{|\hat{\jmath}}\right)\right)\mathbf{h} + \mathbf{B}_1^\perp \underline{\mathbf{D}}\overline{\mathbf{D}}^{-1}\overline{\mathbf{F}_c}\mathbf{h}' + \mathbf{B}_1^\perp \mathbf{R}_c\mathbf{h}' \\
&= \left(\sum_{j=1}^{\alpha} \mathbf{X}_{j,\mathsf{m}^\star_j}^\top + \mathsf{F}\left(\mathsf{m}^\star_{|\hat{\jmath}}\right)\right)\mathbf{h} + \mathbf{B}_1^\perp \mathbf{R}_c\overline{\mathbf{F}_c}^{-1}\mathbf{h}
\end{aligned}$$

with

$$\mathsf{F}\left(\mathsf{m}^\star_{|\hat{\jmath}}\right) := \mathbf{B}_1^\perp \mathsf{ZF}_{\hat{\jmath}}\left(\mathsf{m}^\star_{|\hat{\jmath}}\right)^\top + \mathbf{B}_0^\perp \mathsf{OF}_{\hat{\jmath}}\left(\mathsf{m}^\star_{|\hat{\jmath}}\right)^\top.$$

If $\mathbf{R}_c = \mathbf{0}$, the reduction is simulating $\mathsf{G}_{2,\hat{\jmath},1}$. If $\mathbf{R}_c$ is uniformly random, we implicitly set $\mathsf{ZF}'_{\hat{\jmath}}(\mathsf{m}_{|\hat{\jmath}}) := \mathbf{R}_c\overline{\mathbf{F}_c}^{-1}$ and are simulating game $\mathsf{G}_{2,\hat{\jmath},2}$. □

Lemma 9 ($\mathsf{G}_{2,\hat{\jmath},2} \rightsquigarrow \mathsf{G}_{2,\hat{\jmath},3}$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\jmath},2} \Rightarrow 1\right] - \Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\jmath},3} \Rightarrow 1\right]\right| \leq k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}) + \frac{Q_c + 2}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. We define

$$\mathsf{OF}_{\hat{\jmath}+1}(\mathsf{m}_{|\hat{\jmath}+1}) := \begin{cases} \mathsf{OF}_{\hat{\jmath}}(\mathsf{m}_{|\hat{\jmath}}) + \mathsf{OF}'_{\hat{\jmath}}(\mathsf{m}_{|\hat{\jmath}}) & \text{if } \mathsf{m}_{\hat{\jmath}+1} = 0 \\ \mathsf{OF}_{\hat{\jmath}}(\mathsf{m}_{|\hat{\jmath}}) & \text{if } \mathsf{m}_{\hat{\jmath}+1} = 1 \end{cases},$$

where $\mathsf{OF}'_{\hat{\jmath}} : \{0,1\}^{\hat{\jmath}} \to \mathbb{Z}_q^{1\times k}$ is another independent random function. Since $\mathsf{OF}_{\hat{\jmath}}$ in not used in game $\mathsf{G}_{2,\hat{\jmath},3}$, $\mathsf{OF}_{\hat{\jmath}+1}$ is a random function.

The argument that the games $\mathsf{G}_{2,\hat{\jmath},2}$ and $\mathsf{G}_{2,\hat{\jmath},3}$ are computationally indistinguishable under an MDDH assumption in $\mathbb{G}_1$ is the same as in Lemma 8, just with the roles of 0 and 1 swapped. □

Lemma 10 (Optimization: $\mathsf{G}_{2,\hat{\jmath},1} \rightsquigarrow \mathsf{G}_{2,\hat{\jmath},3}$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\jmath},1} \Rightarrow 1\right] - \Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\jmath},3} \Rightarrow 1\right]\right| \leq k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}) + \frac{Q_c + 2}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. We can do the reduction of Lemmata 8 and 9 in one step using only one MDDH challenge in $\mathbb{G}_1$. This combined reduction embeds the challenge in both $\mathbf{X}_{\hat{\jmath}+1,1}$ as $\mathbf{X}_{\hat{\jmath}+1,1} := \mathbf{J}_{\hat{\jmath}+1,1} + \mathbf{B}_1^\perp \underline{\mathbf{D}} \overline{\mathbf{D}}^{-1}$ and $\mathbf{X}_{\hat{\jmath}+1,0}$ as $\mathbf{X}_{\hat{\jmath}+1,0} := \mathbf{J}_{\hat{\jmath}+1,0} + \mathbf{B}_0^\perp \underline{\mathbf{D}} \overline{\mathbf{D}}^{-1}$ and picks in each CHAL query on $\mathsf{m}^\star$ c as the index of the first CHAL query on a message with prefix $\mathsf{m}^\star_{|\hat{\jmath}+1}$. □

Lemma 11 ($\mathsf{G}_{2,\hat{\jmath},3} \rightsquigarrow \mathsf{G}_{2,\hat{\jmath}+1,0}$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\jmath},3} \Rightarrow 1\right] - \Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\jmath}+1,0} \Rightarrow 1\right]\right| \leq 2k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},2}(\mathcal{B}) + \frac{2}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. In $\mathsf{G}_{2,\hat{\jmath},3}$ we replace the term $\mathsf{ZF}_{\hat{\jmath}+1}\left(\mathsf{m}_{|\hat{\jmath}+1}\right)\left(\mathbf{B}_1^\perp\right)^\top + \mathsf{OF}_{\hat{\jmath}+1}\left(\mathsf{m}_{|\hat{\jmath}+1}\right)\left(\mathbf{B}_0^\perp\right)^\top$ with $\mathsf{RF}_{\hat{\jmath}+1}\left(\mathsf{m}_{|\hat{\jmath}+1}\right)$. This does not change the distribution, since $\mathbf{B}_1^\perp, \mathbf{B}_0^\perp$ is a basis of $\mathbb{Z}_q^{2k}$.

The remaining transition is the reverse of Lemma 7. □

Lemma 12 ($\mathsf{G}_{2,\alpha,0} \rightsquigarrow \mathsf{G}_3$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\alpha,0} \Rightarrow 1\right] - \Pr\left[\mathsf{G}^{\mathcal{A}}_{3} \Rightarrow 1\right]\right| \leq \frac{Q_e}{q^{2k}}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. Assume $Q_e \cap Q_c = \emptyset$; otherwise, the adversary has lost the game regardless of her output. Furthermore assume, that $\mathbf{t} \neq \mathbf{0} \in \mathbb{Z}_q^{2k}$. This happens with probability at least $(1 - 1/q^{2k})$.

In each EVAL query the value $\mathsf{RF}_\alpha(\mathsf{m})\mathbf{t}$ is then distributed like a fresh random vector from $\mathbb{Z}_q^k$ the first time a tag for m is queried. We can ignore duplicated queries for m since they will be answered with the same tag. □

Lemma 13 ($\mathsf{G}_3 \rightsquigarrow \mathsf{G}_4$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{3} \Rightarrow 1\right] - \Pr\left[\mathsf{G}^{\mathcal{A}}_{4} \Rightarrow 1\right]\right| \leq 2k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}) + \frac{2}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. We pick a Q_c fold $\mathcal{U}_{3k,k}$-MDDH challenge $\left([\mathbf{D}]_1, [\mathbf{f}_1]_1, \ldots, [\mathbf{f}_{Q_c}]_1\right)$ and use the reduction given in Figure 7.

Assume that $\overline{\mathbf{D}}$ is invertible. This happens with probability at least $(1 - 1/(q-1))$. Write $\mathbf{f}_c =: \begin{pmatrix} \overline{\mathbf{D}}\mathbf{w}_c \\ \underline{\mathbf{D}}\mathbf{w}_c + \mathbf{r}_c \end{pmatrix}$ where $\mathbf{w}_c$ is uniform random in $\mathbb{Z}_q^k$ and $\mathbf{r}_c$ is $\mathbf{0} \in \mathbb{Z}_q^{2k}$ or uniform random in $\mathbb{Z}_q^{2k}$. Then $\mathbf{h} := \overline{\mathbf{f}_c}$ is a uniform random vector in $\mathbb{Z}_q^k$, since $\overline{\mathbf{D}}$ has full rank and $\mathbf{w}_c$ is uniformly random.

$\underline{\text{INIT}_{\mathsf{MAC}}}$:	$\underline{\text{EVAL}(\mathsf{m} \in \mathcal{S})}$:

parse $\mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
$\mathbf{B}_0, \mathbf{B}_1 \xleftarrow{\$} \mathcal{U}_{2k,k}$
such that $\mathbf{B}_0, \mathbf{B}_1$ is a basis of $\mathbb{Z}_q^{2k}$
for $j \in \{1, \dots, \alpha\},\ b \in \{0,1\}$ **do**
$\quad \mathbf{J}_{j,b} \xleftarrow{\$} \mathbb{Z}_q^{k \times 2k}$
$\quad$ **if** $j \neq 1$ **then** $\mathbf{X}_{j,b} := \mathbf{J}_{j,b}$
// Implicit: For $b \in \{0,1\}$:
// $\mathbf{X}_{1,b} := \mathbf{J}_{1,b} + \left(\underline{\mathbf{D}}\overline{\mathbf{D}}^{-1}\right)^\top$
$\mathbf{x}' \xleftarrow{\$} \mathbb{Z}_q^k$
return $\mathcal{PG}$
	$\mathcal{Q}_\mathcal{M} := \mathcal{Q}_\mathcal{M} \cup \{\mathsf{m}\}$
	$\mathbf{t} := \mathsf{RF}(\mathsf{m}) \in \mathbb{Z}_q^{2k}$
	$\mathbf{u} := \widetilde{\mathsf{RF}}(\mathsf{m})$
	return $\left([\mathbf{t}]_2, [\mathbf{u}]_2\right)$
	
	$\underline{\text{CHAL}(\mathsf{m}^\star \in \mathcal{S})}$:
	$\mathcal{C}_\mathcal{M} := \mathcal{C}_\mathcal{M} \cup \{\mathsf{m}^\star\}$
	Let this be the c-th CHAL query.
	$\mathbf{h} := \overline{\mathbf{f}_c}$
	$\mathbf{h}_0 := \left(\sum_{j=1}^{\alpha} \mathbf{J}_{j,\mathsf{m}_j^\star}^\top + \mathbf{B}_1^\perp \mathsf{RF}_\alpha(\mathsf{m}^\star)^\top\right)\mathbf{h} + \underline{\mathbf{f}_c}$
	$h_1 := (\mathbf{x}')^\top \mathbf{h}$
	return $\left([\mathbf{h}]_1, [\mathbf{h}_0]_1, [h_1]_T\right)$

$\underline{\text{FINALIZE}_{\mathsf{MAC}}(\beta \in \{0,1\})}$: **return** $(\mathcal{C}_\mathcal{M} \cap \mathcal{Q}_\mathcal{M} = \emptyset) \wedge \beta$	

Fig. 7. Reduction for the transition from G_3 to G_4 to the Q_c-fold $\mathcal{U}_{3k,k}$-MDDH challenge $\left([\mathbf{D}]_1, [\mathbf{f}_1]_1, \dots, [\mathbf{f}_{Q_c}]_1\right)$.

The value $\mathbf{h}_0$ is calculated as

$$\begin{aligned}
\mathbf{h}_0 &:= \left(\sum_{j=1}^{\alpha} \mathbf{J}_{j,\mathsf{m}_j^\star}^\top + \mathbf{B}_1^\perp \mathsf{RF}_\alpha(\mathsf{m}^\star)^\top\right)\mathbf{h} + \underline{\mathbf{f}_c} \\
&= \left(\sum_{j=1}^{\alpha} \mathbf{J}_{j,\mathsf{m}_j^\star}^\top + \mathbf{B}_1^\perp \mathsf{RF}_\alpha(\mathsf{m}^\star)^\top\right)\mathbf{h} + \underline{\mathbf{D}}\overline{\mathbf{D}}^{-1}\overline{\mathbf{f}_c} + \mathbf{r}_c \\
&= \left(\sum_{j=1}^{\alpha} \mathbf{X}_{j,\mathsf{m}_j^\star}^\top + \mathbf{B}_1^\perp \mathsf{RF}_\alpha(\mathsf{m}^\star)^\top\right)\mathbf{h} + \mathbf{r}_c\,.
\end{aligned}$$

If $\mathbf{r}_c = \mathbf{0}$, we are simulating game G_3. If $\mathbf{r}_c$ is uniform random, then $\mathbf{h}_0$ is uniform random and we are simulating game G_4. □

Lemma 14 ($\mathsf{G}_4 \rightsquigarrow \mathsf{G}_5$). *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}_4^\mathcal{A} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_5^\mathcal{A} \Rightarrow 1\right]\right| \leq \mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}) + \frac{2}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. We pick a Q_c fold $\mathcal{U}_k$-MDDH challenge $\left([\mathbf{D}]_1, [\mathbf{f}_1]_1, \dots, [\mathbf{f}_{Q_c}]_1\right)$ and use the reduction given in Figure 8.

Assume that $\overline{\mathbf{D}}$ is invertible. This happens with probability at least $(1 - 1/(q-1))$. Write $\mathbf{f}_c =: \begin{pmatrix} \overline{\mathbf{D}}\mathbf{w}_c \\ \underline{\mathbf{D}}\mathbf{w}_c + r_c \end{pmatrix}$ where $\mathbf{w}_c$ is uniform random in $\mathbb{Z}_q^k$ and r_c is 0

$\underline{\text{INIT}_{\mathsf{MAC}}}$:	$\underline{\text{EVAL}(\mathsf{m} \in \mathcal{S})}$:
parse $\mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$	$\mathcal{Q}_\mathcal{M} := \mathcal{Q}_\mathcal{M} \cup \{\mathsf{m}\}$
$\mathbf{B}_0, \mathbf{B}_1 \xleftarrow{\$} \mathcal{U}_{2k,k}$	$\mathbf{t} := \mathsf{RF}(\mathsf{m}) \in \mathbb{Z}_q^{2k}$
such that $\mathbf{B}_0, \mathbf{B}_1$ is a basis of $\mathbb{Z}_q^{2k}$	$\mathbf{u} := \widetilde{\mathsf{RF}}(\mathsf{m})$
for $j \in \{1, \ldots, \alpha\},\ b \in \{0,1\}$ **do**	**return** $\left([\mathbf{t}]_2, [\mathbf{u}]_2\right)$
$\lfloor \mathbf{X}_{j,b} \xleftarrow{\$} \mathbb{Z}_q^{k \times 2k}$	
$\mathbf{j}' \xleftarrow{\$} \mathbb{Z}_q^k$	$\underline{\text{CHAL}(\mathsf{m}^\star \in \mathcal{S})}$:
// Implicit: $\mathbf{x}' := \mathbf{j}' + \left(\underline{\mathbf{D}}\overline{\mathbf{D}}^{-1}\right)^\top$	$\mathcal{C}_\mathcal{M} := \mathcal{C}_\mathcal{M} \cup \{\mathsf{m}^\star\}$
return $\mathcal{PG}$	Let this be the c-th CHAL query.
	$\mathbf{h} := \overline{\mathbf{f}_c}$
$\underline{\text{FINALIZE}_{\mathsf{MAC}}(\beta \in \{0,1\})}$:	$\mathbf{h}_0 \xleftarrow{\$} \mathbb{Z}_q^{2k}$
return $(\mathcal{C}_\mathcal{M} \cap \mathcal{Q}_\mathcal{M} = \emptyset) \wedge \beta$	$h_1 := (\mathbf{j}')^\top \mathbf{h} + \underline{\mathbf{f}_c}$
	return $\left([\mathbf{h}]_1, [\mathbf{h}_0]_1, [h_1]_T\right)$

Fig. 8. Reduction for the transition from G_4 to G_5 to the Q_c-fold $\mathcal{U}_k$-MDDH challenge $\left([\mathbf{D}]_1, [\mathbf{f}_1]_1, \ldots, [\mathbf{f}_{Q_c}]_1\right)$.

or uniform random in $\mathbb{Z}_q$. Then, just like in the previous Lemma, $\mathbf{h} := \overline{\mathbf{f}_c}$ is a uniform random vector in $\mathbb{Z}_q^k$, since $\overline{\mathbf{D}}$ has full rank and $\mathbf{w}_c$ is uniformly random.

The value h_1 is calculated as

$$h_1 := (\mathbf{j}')^\top \mathbf{h} + \underline{\mathbf{f}_c} = (\mathbf{j}')^\top \mathbf{h} + \underline{\mathbf{D}}\overline{\mathbf{D}}^{-1}\overline{\mathbf{f}_c} + r_c = (\mathbf{x}')^\top \mathbf{h} + r_c\,.$$

If $r_c = 0$, we are simulating game G_4. If r_c is uniform random, then h_1 is uniform random and we are simulating game G_5. □

SUMMARY. To prove Theorem 1, we combine Lemmata 5–14 to change $\mathbf{h}_0$ and h_1 from real to random and then apply Lemmata 12–5 in reverse order to undo all changes to the EVAL oracle to get to the $\mathsf{mPR\text{-}CMA}_{\mathsf{rand}}$ game. The Lemmata 8 and 9 resp. Lemma 10 get information theoretic arguments then. □

3.2 Tight Multi-challenge Security for the first LP MAC

Here we show how tight multi-challenge security can be obtained for the first HIBE from [32]. The MAC, given in Figure 9, only differs in the parameter η, that is k here. Furthermore this MAC has identity space base set $\mathcal{S} = \{0,1\}^\alpha$ (for arbitrary $\alpha \in \mathbb{N}_+$) and uses $n = 3k$, $n' = k$, $\ell(p) = 1$ (thus also satisfies the delegatable, affine MAC notion) and $\ell'(l,i) = 2i\alpha$. To match the formal definition, $\mathbf{X}_{i,j,b}$ should be renamed to $\mathbf{X}_{i,2j-b}$ and $f_{i,2j-b}(\mathsf{m}) := \left(\left[\!\left[\mathsf{m}_{|i}\right]\!\right]_j \stackrel{?}{=} b\right)$. In the single-challenge setting, all of these transitions are information-theoretic secure, but in the multi-challenge setting we need a MDDH-assumption in $\mathbb{G}_1$ to proof them.

Theorem 2 (Security of MAC_1). MAC_1 *is tightly* mHPR-CMA *secure under the* $\mathcal{U}_k$-MDDH *assumption for* $\mathbb{G}_1$ *and* $\mathbb{G}_2$. *More precisely, for all adversaries* $\mathcal{A}$

$\underline{\mathsf{Gen}_{\mathsf{MAC}}(\mathbb{G}_2, q, P_2)\text{:}}$
$\mathbf{B} \xleftarrow{\$} \mathcal{U}_{3k,k}$
for $i \in \{1, \dots, L\},\ j \in \{1, \dots, i\alpha\},\ b \in \{0,1\}$ **do** $\mathbf{X}_{i,j,b} \xleftarrow{\$} \mathbb{Z}_q^{k \times 3k}$
$\mathbf{x}' \xleftarrow{\$} \mathbb{Z}_q^k$
return $\mathsf{sk}_{\mathsf{MAC}} := \left(\mathbf{B}, (\mathbf{X}_{i,j,b})_{1 \le i \le L, 1 \le j \le i\alpha, b \in \{0,1\}}, \mathbf{x}'\right)$

$\underline{\mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m} \in \mathcal{S}^p)\text{:}}$
parse $\mathsf{sk}_{\mathsf{MAC}} =: \left(\mathbf{B}, (\mathbf{X}_{i,j,b})_{1 \le i \le L, 1 \le j \le i\alpha, b \in \{0,1\}}, \mathbf{x}'\right)$
$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k;\ \mathbf{t} := \mathbf{B}\mathbf{s}$
$\mathbf{u} := \sum_{i=1}^{p} \sum_{j=1}^{i\alpha} \mathbf{X}_{i,j,[\![\mathsf{m}]\!]_j} \mathbf{t} + \mathbf{x}'$
return $\left([\mathbf{t}]_2, [\mathbf{u}]_2\right)$

$\underline{\mathsf{Ver}_{\mathsf{MAC}}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m} \in \mathcal{S}^p, \tau)\text{:}}$
parse $\mathsf{sk}_{\mathsf{MAC}} =: \left(\mathbf{B}, (\mathbf{X}_{i,j,b})_{1 \le i \le L, 1 \le j \le i\alpha, b \in \{0,1\}}, \mathbf{x}'\right)$
parse $\tau =: \left([\mathbf{t}]_2, [\mathbf{u}]_2\right)$
return $\mathbf{u} \stackrel{?}{=} \sum_{i=1}^{p} \sum_{j=1}^{i\alpha} \mathbf{X}_{i,j,[\![\mathsf{m}]\!]_j} \mathbf{t} + \mathbf{x}'$

Fig. 9. The new multi-challenge tightly secure delegatable affine MAC MAC_1.

there exist adversaries $\mathcal{B}_1$ *and* $\mathcal{B}_2$ *with*

$$\begin{aligned}\mathsf{Adv}^{\mathsf{mhpr\text{-}cma}}_{\mathsf{MAC}_1,\mathsf{PGGen}}(\mathcal{A}) \le{}& \left(8k(\alpha+1)L + 8k\alpha L^2\right)\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},2}(\mathcal{B}_1)\\ &+ \left(1 + k(\alpha+4)L + k\alpha L^2\right)\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}_2)\\ &+ \frac{10 + 2Q_c + (Q_c+6)\alpha\left(L^2+L\right)}{q-1} + \frac{2Q_e}{q^{2k}}\end{aligned}$$

and $T(\mathcal{B}_1) \approx T(\mathcal{B}_2) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$*, where* Q_e *resp.* Q_c *denotes the number of* Eval *resp.* Chal *queries of* $\mathcal{A}$ *and* poly *is a polynomial independent of* $\mathcal{A}$*.*

The proof can be found in Appendix A.1. A summary of the hybrids can be found in Table 4.

3.3 Tight Multi-challenge Security for the second LP MAC

The second MAC of [32] can be made tightly secure in a similar way to the first MAC. Details can be found in Appendix B.

4 Anonymous Delegatable Affine MACs

A proof that MAC_1 is suitable for constructing an anonymous HIBE can be found in Appendix C.

Hybrid	$\mathbf{t}$ uniform in	$r_{\mathbf{u}}(\mathsf{m})$	$r_{\mathbf{h}_0}(\mathsf{m})$	Transition
G_0	$\mathsf{Span}(\mathbf{B})$	0		Original game
G_1	$\mathsf{Span}(\mathbf{B})$	0		Identical
$\mathsf{G}_{2,\hat{\imath},0}$	$\mathsf{Span}(\mathbf{B})$	0		Identical
$\mathsf{G}_{2,\hat{\imath},1}$	$\mathbb{Z}_q^{3k}$	0		$\mathcal{U}_k$-MDDH in $\mathbb{G}_2$
$\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},0}$	$\mathbb{Z}_q^{3k}$	$\mathsf{RF}_{\hat{\imath},\hat{\jmath}}\big([\![\mathsf{m}]\!]_{\mid\hat{\jmath}}\big)\big(\mathbf{B}^{\perp}\big)^{\top}$		Identical
$\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},1}$	**if** $[\![\mathsf{m}]\!]_{\hat{\jmath}+1}=0$ **then** $\mid \mathsf{Span}(\mathbf{B}\mid\mathbf{B}_0)$ **else** $\lfloor \mathsf{Span}(\mathbf{B}\mid\mathbf{B}_1)$	$\mathsf{RF}_{\hat{\imath},\hat{\jmath}}\big([\![\mathsf{m}]\!]_{\mid\hat{\jmath}}\big)\big(\mathbf{B}^{\perp}\big)^{\top}$		$\mathcal{U}_k$-MDDH in $\mathbb{G}_2$
$\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},2}$		$\big(\mathsf{ZF}_{\hat{\imath},\hat{\jmath}+1}\big([\![\mathsf{m}]\!]_{\mid\hat{\jmath}+1}\big)(\mathbf{B}_0^*)^{\top} + \mathsf{OF}_{\hat{\imath},\hat{\jmath}}\big([\![\mathsf{m}]\!]_{\mid\hat{\jmath}}\big)(\mathbf{B}_1^*)^{\top}\big)$		$\mathcal{U}_k$-MDDH in $\mathbb{G}_1$
$\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},3}$		$\big(\mathsf{ZF}_{\hat{\imath},\hat{\jmath}+1}\big([\![\mathsf{m}]\!]_{\mid\hat{\jmath}+1}\big)(\mathbf{B}_0^*)^{\top} + \mathsf{OF}_{\hat{\imath},\hat{\jmath}+1}\big([\![\mathsf{m}]\!]_{\mid\hat{\jmath}+1}\big)(\mathbf{B}_1^*)^{\top}\big)$		$\mathcal{U}_k$-MDDH in $\mathbb{G}_1$
$\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath}+1,0}$	$\mathbb{Z}_q^{3k}$	$\mathsf{RF}_{\hat{\imath},\hat{\jmath}+1}\big([\![\mathsf{m}]\!]_{\mid\hat{\jmath}+1}\big)\big(\mathbf{B}^{\perp}\big)^{\top}$		$\mathcal{U}_k$-MDDH in $\mathbb{G}_2$
$\mathsf{G}_{2,\hat{\imath},3}$	$\mathbb{Z}_q^{3k}$	uniform random	$\mathsf{RF}_{\hat{\imath}}\big(\mathsf{m}_{\mid\hat{\imath}}\big)\big(\mathbf{B}^{\perp}\big)^{\top}$	Statistically close
$\mathsf{G}_{2,\hat{\imath},4}$	$\mathbb{Z}_q^{3k}$	uniform random	0	$\mathcal{U}_k$-MDDH in $\mathbb{G}_1$
$\mathsf{G}_{2,\hat{\imath},5}$	$\mathsf{Span}(\mathbf{B})$	uniform random	0	$\mathcal{U}_k$-MDDH in $\mathbb{G}_2$
G_3	$\mathsf{Span}(\mathbf{B})$	uniform random	0	$\mathcal{U}_k$-MDDH in $\mathbb{G}_1$

Table 4. Summary of the hybrids for the security proof of Theorem 2. Non-duplicated EVAL queries (with $p=\hat{\imath}$) draw $\mathbf{t}$ from the set described by the second column and add the randomness $r_{\mathbf{u}}(\mathsf{m})\mathbf{t}$ to $\mathbf{u}$ or choose $\mathbf{u}$ uniform random. The CHAL queries add the term $r_{\mathbf{h}_0}(\mathsf{m}^\star)^\top\mathbf{h}$ to $\mathbf{h}_0$ (if $\mathsf{m}^\star$ has length $\geq\hat{\imath}$). The column "Transition" displays how we can switch to this hybrid from the previous one. The background colors indicate repeated transitions.

5 Transformation to HIBE

Any mHPR-CMA affine MAC with levels can be tightly transformed to an hierarchical identity-based key encapsulation mechanism (HIBKEM) under the $\mathcal{D}_{k+\eta,k}$-MDDH assumption in $\mathbb{G}_1$ with the transformation given in Figure 10. The transformation follows the same idea as [5]. A security proof can be found in Appendix D.2. With a QANIZK for linear subspaces we can use the idea of [25] to obtain an IND-HID-CCA-secure HIBE. Details can be found in Appendix D.3.

The anonymity-preserving variants of these transformations for mAPR-CMA-secure delegatable affine MACs can be found in Appendix E.

6 Instantiations

The resulting HIBEs can be instantiated with any MDDH assumption. The result for both general MDDH assumptions and the SXDH assumption can be found in Appendix F.

$\underline{\mathsf{Gen}(1^\lambda)}$:
$\mathcal{PG} \xleftarrow{\$} \mathsf{PGGen}(1^\lambda)$
parse $\mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
$\mathsf{sk}_{\mathsf{MAC}} \xleftarrow{\$} \mathsf{Gen}_{\mathsf{MAC}}(\mathbb{G}_2, q, P_2)$
$\mathsf{sk}_{\mathsf{MAC}} =: \left(\mathbf{B}, (\mathbf{X}_{l,i,j})_{\substack{1\le l\le \ell(p), 1\le i\le L,,\\ 1\le j\le \ell'(l,i)}}, \mathbf{x}'\right)$
$\mathbf{A} \xleftarrow{\$} \mathcal{D}_{k+\eta,k}$
for $l \in \{1,\dots,\ell(L)\},\ i \in \{1,\dots,L\},\ j \in \{1,\dots,\ell'(l,i)\}$ **do**
  $\mathbf{Y}_{l,i,j} \xleftarrow{\$} \mathbb{Z}_q^{k\times n};\ \mathbf{Z}_{l,i,j} := \left(\mathbf{Y}_{l,i,j}^\top \mid \mathbf{X}_{l,i,j}^\top\right)\mathbf{A}$
  $\mathbf{D}_{l,i,j} := \mathbf{X}_{l,i,j} \cdot \mathbf{B};\ \mathbf{E}_{l,i,j} := \mathbf{Y}_{l,i,j} \cdot \mathbf{B}$
$\mathbf{y}' \xleftarrow{\$} \mathbb{Z}_q^k;\ \mathbf{z}' := \left(\mathbf{y}'^\top \mid \mathbf{x}'^\top\right) \cdot \mathbf{A}$
$\widetilde{\mathbf{Z}} := \left([\mathbf{Z}_{l,i,j}]_1\right)_{1\le l\le \ell(p), 1\le i\le L, 1\le j\le \ell'(l,i)}$
$\mathsf{pk} := \left(\mathcal{PG}, [\mathbf{A}]_1, \widetilde{\mathbf{Z}}, [\mathbf{z}']_1\right)$
$\widetilde{\mathsf{dk}} := \left([\mathbf{D}_{l,i,j}]_2, [\mathbf{E}_{l,i,j}]_2\right)_{\substack{1\le l\le \ell(p), 1\le i\le L,\\ 1\le j\le \ell'(l,i)}}$
$\mathsf{dk} := \left([\mathbf{B}]_2, \widetilde{\mathsf{dk}}\right)$
$\mathsf{sk} := \left(\mathsf{sk}_{\mathsf{MAC}}, (\mathbf{Y}_{l,i,j})_{\substack{1\le l\le \ell(p), 1\le i\le L,,\\ 1\le j\le \ell'(l,i)}}, \mathbf{y}'\right)$
return $(\mathsf{pk}, \mathsf{dk}, \mathsf{sk})$

$\underline{\mathsf{Ext}(\mathsf{sk}, \mathsf{id} \in \mathcal{S}^p)}$:
$\left(\left([\mathbf{t}_l]_2\right)_{1\le l\le \ell(p)}, [\mathbf{u}]_2\right) \xleftarrow{\$} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{id})$
$\mathbf{v} := \sum_{l=1}^{\ell(p)} \left(\sum_{i=1}^{p} \sum_{j=1}^{\ell'(l,i)} f_{l,i,j}\left(\mathsf{id}_{|i}\right)\mathbf{Y}_{l,i,j} \right)\mathbf{t}_l + \mathbf{y}'$
for $l \in \{1,\dots,\ell(p)\},\ i \in \{p+1,\dots,L\},\ j \in \{1,\dots,\ell'(l,i)\}$ **do**
  $\mathbf{d}_{l,i,j} := \mathbf{X}_{l,i,j}\mathbf{t}_l;\ \mathbf{e}_{l,i,j} := \mathbf{Y}_{l,i,j}\mathbf{t}_l$
$\mathsf{usk}[\mathsf{id}] := \left(\left([\mathbf{t}_l]_2\right)_{1\le l\le \ell(p)}, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$
$\mathsf{udk}[\mathsf{id}] := \left([\mathbf{d}_{l,i,j}]_2, [\mathbf{e}_{l,i,j}]_2\right)_{\substack{1\le l\le \ell(p),\\ p+1\le i\le L,\\ 1\le j\le \ell'(l,i)}}$
return $(\mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}])$

$\underline{\mathsf{Enc}(\mathsf{pk}, \mathsf{id} \in \mathcal{S}^p)}$:
$\mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^k;\ \mathbf{c}_0 := \mathbf{A}\mathbf{r}$
for $l \in \{1,\dots,\ell(p)\}$ **do**
  $\mathbf{c}_{1,l} := \sum_{i=1}^{p} \sum_{j=1}^{\ell'(l,i)} f_{l,i,j}\left(\mathsf{id}_{|i}\right)\mathbf{Z}_{l,i,j}\mathbf{r}$
$\mathsf{C} := \left([\mathbf{c}_0]_1, \left([\mathbf{c}_{1,l}]_1\right)_{1\le l\le \ell(p)}\right)$
$\mathsf{K} := \mathbf{z}' \cdot \mathbf{r}$
return $\left([\mathsf{K}]_T, \mathsf{C}\right)$

$\underline{\mathsf{Del}(\mathsf{dk}, \mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}], \mathsf{id} \in \mathcal{S}^p, \mathsf{id}_{p+1})}$:
$\mathsf{usk}[\mathsf{id}] =: \left(\left([\mathbf{t}_l]_2\right)_{1\le l\le \ell(p)}, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$
$\mathsf{udk}[\mathsf{id}] =: \left([\mathbf{d}_{l,i,j}]_2, [\mathbf{e}_{l,i,j}]_2\right)_{\substack{1\le l\le \ell(p),\\ p+1\le i\le L,\\ 1\le j\le \ell'(l,i)}}$
for $l \in \{\ell(p)+1,\dots,\ell(p+1)\}$ **do**
  $\mathbf{t}_l := \mathbf{0}$
for $l \in \{1,\dots,\ell(p+1)\}$ **do**
  $\mathbf{s}'_l \xleftarrow{\$} \mathbb{Z}_q^{n'};\ \mathbf{t}'_l := \mathbf{t}_l + \mathbf{B}\mathbf{s}'_l$
$\mathsf{id}' := (\mathsf{id}_1, \dots, \mathsf{id}_p, \mathsf{id}_{p+1})$
$\mathbf{u}' := \mathbf{u} + \sum_{l=1}^{\ell(p)} \sum_{j=1}^{\ell'(l,p+1)} f_{l,p+1,j}(\mathsf{id}')\mathbf{d}_{l,p+1,j}$
  $+ \sum_{l=1}^{\ell(p+1)} \left(\sum_{i=1}^{p+1} \sum_{j=1}^{\ell'(l,i)} f_{l,i,j}\left(\mathsf{id}'_{|i}\right)\mathbf{D}_{l,i,j} \right)\mathbf{s}'_l$
$\mathbf{v}' := \mathbf{v} + \sum_{l=1}^{\ell(p)} \sum_{j=1}^{\ell'(l,p+1)} f_{l,p+1,j}(\mathsf{id}')\mathbf{e}_{l,p+1,j}$
  $+ \sum_{l=1}^{\ell(p+1)} \left(\sum_{i=1}^{p+1} \sum_{j=1}^{\ell'(l,i)} f_{l,i,j}\left(\mathsf{id}'_{|i}\right)\mathbf{E}_{l,i,j} \right)\mathbf{s}'_l$
for $l \in \{1,\dots,\ell(p)\},\ i \in \{p+2,\dots,\dots,L\},\ j \in \{1,\dots,\ell'(l,i)\}$ **do**
  $\mathbf{d}'_{l,i,j} := \mathbf{d}_{l,i,j} + \mathbf{D}_{l,i,j}\mathbf{s}'_l$
  $\mathbf{e}'_{l,i,j} := \mathbf{e}_{l,i,j} + \mathbf{E}_{l,i,j}\mathbf{s}'_l$
for $l \in \{\ell(p)+1,\dots,\ell(p+1)\},\ i \in \{p+2,\dots,L\},\ j \in \{1,\dots,\ell'(l,i)\}$ **do**
  $\mathbf{d}'_{l,i,j} := \mathbf{D}_{l,i,j}\mathbf{s}'_l;\ \mathbf{e}'_{l,i,j} := \mathbf{E}_{l,i,j}\mathbf{s}'_l$
$\mathsf{usk}' := \left(\left([\mathbf{t}'_l]_2\right)_{1\le l\le \ell(p+1)}, [\mathbf{u}']_2, [\mathbf{v}']_2\right)$
$\mathsf{udk}' := \left(\left[\mathbf{d}'_{l,i,j}\right]_2, \left[\mathbf{e}'_{l,i,j}\right]_2\right)_{\substack{1\le l\le \ell(p+1),\\ p+2\le i\le L,\\ 1\le j\le \ell'(l,i)}}$
return $(\mathsf{usk}', \mathsf{udk}')$

$\underline{\mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id} \in \mathcal{S}^p, \mathsf{C})}$:
$\mathsf{usk}[\mathsf{id}] =: \left(\left([\mathbf{t}_l]_2\right)_{1\le l\le \ell(p)}, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$
parse $\mathsf{C} =: \left([\mathbf{c}_0]_1, \left([\mathbf{c}_{1,l}]_1\right)_{1\le l\le \ell(p)}\right)$
$[\mathsf{K}]_T := e\left(\left[\mathbf{c}_0^\top\right]_1, \begin{bmatrix}\mathbf{v}\\ \mathbf{u}\end{bmatrix}_2\right) - \sum_{l=1}^{\ell(p)} e\left(\left[\mathbf{c}_{1,l}^\top\right]_1, [\mathbf{t}_l]_2\right)$
return $[\mathsf{K}]_T$

Fig. 10. The Transformation $\mathsf{HIBKEM}_{\mathsf{CPA}}$ of an affine MAC with levels to an HIBKEM.

References

1. Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Kohno, T., Lange, T., Malone-Lee, J., Neven, G., Paillier, P., Shi, H.: Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions. In: Shoup, V. (ed.) Advances in Cryptology – CRYPTO 2005. Lecture Notes in Computer Science, vol. 3621, pp. 205–222. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 14–18, 2005) 3
2. Abe, M., Jutla, C.S., Ohkubo, M., Pan, J., Roy, A., Wang, Y.: Shorter QA-NIZK and SPS with tighter security. In: Galbraith, S.D., Moriai, S. (eds.) Advances in Cryptology – ASIACRYPT 2019, Part III. Lecture Notes in Computer Science, vol. 11923, pp. 669–699. Springer, Heidelberg, Germany, Kobe, Japan (Dec 8–12, 2019) 4
3. Attrapadung, N., Hanaoka, G., Yamada, S.: A framework for identity-based encryption with almost tight security. In: Iwata, T., Cheon, J.H. (eds.) Advances in Cryptology – ASIACRYPT 2015, Part I. Lecture Notes in Computer Science, vol. 9452, pp. 521–549. Springer, Heidelberg, Germany, Auckland, New Zealand (Nov 30 – Dec 3, 2015) 9, 10, 17
4. Bellare, M., Goldwasser, S.: New paradigms for digital signatures and message authentication based on non-interative zero knowledge proofs. In: Brassard, G. (ed.) Advances in Cryptology – CRYPTO'89. Lecture Notes in Computer Science, vol. 435, pp. 194–211. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 20–24, 1990) 5
5. Blazy, O., Kiltz, E., Pan, J.: (Hierarchical) identity-based encryption from affine message authentication. In: Garay, J.A., Gennaro, R. (eds.) Advances in Cryptology – CRYPTO 2014, Part I. Lecture Notes in Computer Science, vol. 8616, pp. 408–425. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 17–21, 2014) 2, 3, 4, 5, 10, 11, 17, 27, 51, 52, 53, 77
6. Blazy, O., Kiltz, E., Pan, J.: (Hierarchical) identity-based encryption from affine message authentication. Cryptology ePrint Archive, Report 2014/581 (2014), http://eprint.iacr.org/2014/581 2
7. Boneh, D., Franklin, M.K.: Identity-based encryption from the Weil pairing. In: Kilian, J. (ed.) Advances in Cryptology – CRYPTO 2001. Lecture Notes in Computer Science, vol. 2139, pp. 213–229. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 19–23, 2001) 5
8. Boyen, X., Waters, B.: Anonymous hierarchical identity-based encryption (without random oracles). In: Dwork, C. (ed.) Advances in Cryptology – CRYPTO 2006. Lecture Notes in Computer Science, vol. 4117, pp. 290–307. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 20–24, 2006) 53
9. Canetti, R., Halevi, S., Katz, J.: Chosen-ciphertext security from identity-based encryption. In: Cachin, C., Camenisch, J. (eds.) Advances in Cryptology – EUROCRYPT 2004. Lecture Notes in Computer Science, vol. 3027, pp. 207–222. Springer, Heidelberg, Germany, Interlaken, Switzerland (May 2–6, 2004) 68
10. Chen, J., Wee, H.: Fully, (almost) tightly secure IBE and dual system groups. In: Canetti, R., Garay, J.A. (eds.) Advances in Cryptology – CRYPTO 2013, Part II. Lecture Notes in Computer Science, vol. 8043, pp. 435–460. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 18–22, 2013) 2, 4, 5, 17
11. Dodis, Y., Kiltz, E., Pietrzak, K., Wichs, D.: Message authentication, revisited. In: Pointcheval, D., Johansson, T. (eds.) Advances in Cryptology – EUROCRYPT 2012. Lecture Notes in Computer Science, vol. 7237, pp. 355–374. Springer, Heidelberg, Germany, Cambridge, UK (Apr 15–19, 2012) 6

12. Ducas, L.: Anonymity from asymmetry: New constructions for anonymous HIBE. In: Pieprzyk, J. (ed.) Topics in Cryptology – CT-RSA 2010. Lecture Notes in Computer Science, vol. 5985, pp. 148–164. Springer, Heidelberg, Germany, San Francisco, CA, USA (Mar 1–5, 2010) 53
13. Escala, A., Herold, G., Kiltz, E., Ràfols, C., Villar, J.: An algebraic framework for Diffie-Hellman assumptions. In: Canetti, R., Garay, J.A. (eds.) Advances in Cryptology – CRYPTO 2013, Part II. Lecture Notes in Computer Science, vol. 8043, pp. 129–147. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 18–22, 2013) 3, 6, 11, 12, 13
14. Gay, R., Hofheinz, D., Kiltz, E., Wee, H.: Tightly CCA-secure encryption without pairings. In: Fischlin, M., Coron, J.S. (eds.) Advances in Cryptology – EUROCRYPT 2016, Part I. Lecture Notes in Computer Science, vol. 9665, pp. 1–27. Springer, Heidelberg, Germany, Vienna, Austria (May 8–12, 2016) 2, 12, 70, 72
15. Gay, R., Hofheinz, D., Kohl, L.: Kurosawa-desmedt meets tight security. In: Katz, J., Shacham, H. (eds.) Advances in Cryptology – CRYPTO 2017, Part III. Lecture Notes in Computer Science, vol. 10403, pp. 133–160. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 20–24, 2017) 2
16. Gay, R., Hofheinz, D., Kohl, L., Pan, J.: More efficient (almost) tightly secure structure-preserving signatures. In: Nielsen, J.B., Rijmen, V. (eds.) Advances in Cryptology – EUROCRYPT 2018, Part II. Lecture Notes in Computer Science, vol. 10821, pp. 230–258. Springer, Heidelberg, Germany, Tel Aviv, Israel (Apr 29 – May 3, 2018) 2
17. Gentry, C., Silverberg, A.: Hierarchical ID-based cryptography. In: Zheng, Y. (ed.) Advances in Cryptology – ASIACRYPT 2002. Lecture Notes in Computer Science, vol. 2501, pp. 548–566. Springer, Heidelberg, Germany, Queenstown, New Zealand (Dec 1–5, 2002) 2
18. Gjøsteen, K., Jager, T.: Practical and tightly-secure digital signatures and authenticated key exchange. In: Shacham, H., Boldyreva, A. (eds.) Advances in Cryptology – CRYPTO 2018, Part II. Lecture Notes in Computer Science, vol. 10992, pp. 95–125. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 19–23, 2018) 2
19. Gong, J., Cao, Z., Tang, S., Chen, J.: Extended dual system group and shorter unbounded hierarchical identity based encryption. Designs, Codes and Cryptography 80(3), 525–559 (Sep 2016), https://doi.org/10.1007/s10623-015-0117-z 4
20. Gong, J., Chen, J., Dong, X., Cao, Z., Tang, S.: Extended nested dual system groups, revisited. In: Cheng, C.M., Chung, K.M., Persiano, G., Yang, B.Y. (eds.) PKC 2016: 19th International Conference on Theory and Practice of Public Key Cryptography, Part I. Lecture Notes in Computer Science, vol. 9614, pp. 133–163. Springer, Heidelberg, Germany, Taipei, Taiwan (Mar 6–9, 2016) 3, 9, 10, 17
21. Gong, J., Dong, X., Chen, J., Cao, Z.: Efficient IBE with tight reduction to standard assumption in the multi-challenge setting. In: Cheon, J.H., Takagi, T. (eds.) Advances in Cryptology – ASIACRYPT 2016, Part II. Lecture Notes in Computer Science, vol. 10032, pp. 624–654. Springer, Heidelberg, Germany, Hanoi, Vietnam (Dec 4–8, 2016) 3, 9, 10, 17
22. Groth, J., Sahai, A.: Efficient non-interactive proof systems for bilinear groups. In: Smart, N.P. (ed.) Advances in Cryptology – EUROCRYPT 2008. Lecture Notes in Computer Science, vol. 4965, pp. 415–432. Springer, Heidelberg, Germany, Istanbul, Turkey (Apr 13–17, 2008) 5
23. Hofheinz, D.: Adaptive partitioning. In: Coron, J., Nielsen, J.B. (eds.) Advances in Cryptology – EUROCRYPT 2017, Part III. Lecture Notes in Computer Science, vol. 10212, pp. 489–518. Springer, Heidelberg, Germany, Paris, France (Apr 30 – May 4, 2017) 2

24. Hofheinz, D., Jager, T.: Tightly secure signatures and public-key encryption. In: Safavi-Naini, R., Canetti, R. (eds.) Advances in Cryptology – CRYPTO 2012. Lecture Notes in Computer Science, vol. 7417, pp. 590–607. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 19–23, 2012) 2
25. Hofheinz, D., Jia, D., Pan, J.: Identity-based encryption tightly secure under chosen-ciphertext attacks. In: Peyrin, T., Galbraith, S. (eds.) Advances in Cryptology – ASIACRYPT 2018, Part II. Lecture Notes in Computer Science, vol. 11273, pp. 190–220. Springer, Heidelberg, Germany, Brisbane, Queensland, Australia (Dec 2–6, 2018) 3, 4, 9, 10, 16, 17, 27, 68, 70, 72, 81, 83
26. Hofheinz, D., Kiltz, E.: Secure hybrid encryption from weakened key encapsulation. In: Menezes, A. (ed.) Advances in Cryptology – CRYPTO 2007. Lecture Notes in Computer Science, vol. 4622, pp. 553–571. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 19–23, 2007) 61, 68, 72
27. Hofheinz, D., Koch, J., Striecks, C.: Identity-based encryption with (almost) tight security in the multi-instance, multi-ciphertext setting. In: Katz, J. (ed.) PKC 2015: 18th International Conference on Theory and Practice of Public Key Cryptography. Lecture Notes in Computer Science, vol. 9020, pp. 799–822. Springer, Heidelberg, Germany, Gaithersburg, MD, USA (Mar 30 – Apr 1, 2015) 3, 9, 10
28. Horwitz, J., Lynn, B.: Toward hierarchical identity-based encryption. In: Knudsen, L.R. (ed.) Advances in Cryptology – EUROCRYPT 2002. Lecture Notes in Computer Science, vol. 2332, pp. 466–481. Springer, Heidelberg, Germany, Amsterdam, The Netherlands (Apr 28 – May 2, 2002) 2
29. Jutla, C.S., Roy, A.: Shorter quasi-adaptive NIZK proofs for linear subspaces. In: Sako, K., Sarkar, P. (eds.) Advances in Cryptology – ASIACRYPT 2013, Part I. Lecture Notes in Computer Science, vol. 8269, pp. 1–20. Springer, Heidelberg, Germany, Bengalore, India (Dec 1–5, 2013) 4, 68
30. Kiltz, E., Loss, J., Pan, J.: Tightly-secure signatures from five-move identification protocols. In: Takagi, T., Peyrin, T. (eds.) Advances in Cryptology – ASIACRYPT 2017, Part III. Lecture Notes in Computer Science, vol. 10626, pp. 68–94. Springer, Heidelberg, Germany, Hong Kong, China (Dec 3–7, 2017) 2
31. Kiltz, E., Wee, H.: Quasi-adaptive NIZK for linear subspaces revisited. In: Oswald, E., Fischlin, M. (eds.) Advances in Cryptology – EUROCRYPT 2015, Part II. Lecture Notes in Computer Science, vol. 9057, pp. 101–128. Springer, Heidelberg, Germany, Sofia, Bulgaria (Apr 26–30, 2015) 4
32. Langrehr, R., Pan, J.: Tightly secure hierarchical identity-based encryption. In: Lin, D., Sako, K. (eds.) PKC 2019: 22nd International Conference on Theory and Practice of Public Key Cryptography, Part I. Lecture Notes in Computer Science, vol. 11442, pp. 436–465. Springer, Heidelberg, Germany, Beijing, China (Apr 14–17, 2019) 2, 3, 4, 5, 7, 9, 10, 25, 26, 44, 53, 63
33. Langrehr, R., Pan, J.: Tightly secure hierarchical identity-based encryption. Cryptology ePrint Archive, Report 2019/058 (2019), https://eprint.iacr.org/2019/058 2
34. Langrehr, R., Pan, J.: Hierarchical identity-based encryption with tight multi-challenge security. In: PKC 2020 (To appear) (2020) 1
35. Lewko, A.B.: Tools for simulating features of composite order bilinear groups in the prime order setting. In: Pointcheval, D., Johansson, T. (eds.) Advances in Cryptology – EUROCRYPT 2012. Lecture Notes in Computer Science, vol. 7237, pp. 318–335. Springer, Heidelberg, Germany, Cambridge, UK (Apr 15–19, 2012) 3, 4

36. Lewko, A.B., Waters, B.: New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In: Micciancio, D. (ed.) TCC 2010: 7th Theory of Cryptography Conference. Lecture Notes in Computer Science, vol. 5978, pp. 455–479. Springer, Heidelberg, Germany, Zurich, Switzerland (Feb 9–11, 2010) 3
37. Lewko, A.B., Waters, B.: Why proving HIBE systems secure is difficult. In: Nguyen, P.Q., Oswald, E. (eds.) Advances in Cryptology – EUROCRYPT 2014. Lecture Notes in Computer Science, vol. 8441, pp. 58–76. Springer, Heidelberg, Germany, Copenhagen, Denmark (May 11–15, 2014) 2
38. Naor, M., Reingold, O.: On the construction of pseudo-random permutations: Luby-Rackoff revisited (extended abstract). In: 29th Annual ACM Symposium on Theory of Computing. pp. 189–199. ACM Press, El Paso, TX, USA (May 4–6, 1997) 5
39. Okamoto, T., Takashima, K.: Fully secure unbounded inner-product and attribute-based encryption. In: Wang, X., Sako, K. (eds.) Advances in Cryptology – ASIACRYPT 2012. Lecture Notes in Computer Science, vol. 7658, pp. 349–366. Springer, Heidelberg, Germany, Beijing, China (Dec 2–6, 2012) 53
40. Shi, E., Waters, B.: Delegating capabilities in predicate encryption systems. In: Aceto, L., Damgård, I., Goldberg, L.A., Halldórsson, M.M., Ingólfsdóttir, A., Walukiewicz, I. (eds.) ICALP 2008: 35th International Colloquium on Automata, Languages and Programming, Part II. Lecture Notes in Computer Science, vol. 5126, pp. 560–578. Springer, Heidelberg, Germany, Reykjavik, Iceland (Jul 7–11, 2008) 62
41. Waters, B.: Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In: Halevi, S. (ed.) Advances in Cryptology – CRYPTO 2009. Lecture Notes in Computer Science, vol. 5677, pp. 619–636. Springer, Heidelberg, Germany, Santa Barbara, CA, USA (Aug 16–20, 2009) 4
42. Waters, B.R.: Efficient identity-based encryption without random oracles. In: Cramer, R. (ed.) Advances in Cryptology – EUROCRYPT 2005. Lecture Notes in Computer Science, vol. 3494, pp. 114–127. Springer, Heidelberg, Germany, Aarhus, Denmark (May 22–26, 2005) 3, 4

Supplementary Material

A Omitted Proofs

Proof (of Lemma 4). We calculate the probability by counting the number of column vectors that can be added successively to a $k \times n$ matrix with $n \in \{0, \ldots, k-1\}$ without losing full rank:

$$\frac{\left|\mathbb{Z}_q^{k\times k} \setminus \mathsf{GL}_k(\mathbb{Z}_q)\right|}{\left|\mathbb{Z}_q^{k\times k}\right|} = \frac{1}{q^k} + \frac{q}{q^k} + \cdots + \frac{q^{k-1}}{q^k} = \frac{1+q+\cdots+q^{k-1}}{q^k}$$
$$= \frac{q^k-1}{q^k(q-1)} = \frac{1}{q-1} - \frac{1}{q^k(q-1)} \leq \frac{1}{q-1}$$

□

Proof (of Lemma 7). We first switch to an intermediate hybrid where EVAL queries with $\mathsf{m}_{\hat{\jmath}+1} = 0$ are distributed as in $\mathsf{G}_{2,\hat{\jmath},1}$ and EVAL queries with $\mathsf{m}_{\hat{\jmath}+1} = 1$ are distributed as in $\mathsf{G}_{2,\hat{\jmath},0}$. Therefore use a Q_e-fold $\mathcal{U}_{2k,k}$-MDDH challenge on $\mathbf{B}_0$ in $\mathbb{G}_2$ to switch in EVAL queries $\mathbf{t}$ from uniform random in $\mathbb{Z}_q^{2k}$ to $\mathsf{Span}(\mathbf{B}_0)$ if $\mathsf{m}_{\hat{\jmath}+1} = 0$. During the reduction, only $[\mathbf{B}_0]_2$ and not $\mathbf{B}_0$ is known, but this is sufficient to answer all oracle queries. The column vectors of $\mathbf{B}_0$ and $\mathbf{B}_1$ form a basis of $\mathbb{Z}_q^{2k}$ iff the kernels of $\mathbf{B}_0^\top$ and $\mathbf{B}_1^\top$ are disjoint. This is the case iff all column vectors $\mathbf{b}$ of $\mathbf{B}_1^\perp$ satisfy $\mathbf{B}_0^\top \mathbf{b} \neq \mathbf{0}$. The later can be tested in the group, so the reduction can still ensure that $\mathbf{B}_0, \mathbf{B}_1$ is a basis of $\mathbb{Z}_q^{2k}$, by generating new $\mathbf{B}_1$ until the condition from above is satisfied.

After this we can switch from the intermediate hybrid to $\mathsf{G}_{2,\hat{\jmath},1}$ using another Q_e-fold $\mathcal{U}_{2k,k}$-MDDH challenge on $\mathbf{B}_1$ to switch $\mathbf{t}$ from $\mathbb{Z}_q^{2k}$ to $\mathsf{Span}(\mathbf{B}_1)$ if $\mathsf{m}_{\hat{\jmath}+1} = 1$. The argument is the same as before, just with the roles of 0 and 1 swapped.

By Lemma 3 the Q_e-fold $\mathcal{U}_{2k,k}$-MDDH assumption is at most k times harder then the $\mathcal{U}_{2k,k}$-MDDH assumption, which is equivalent to the $\mathcal{U}_k$-MDDH by Lemma 1. □

A.1 Security Proof for MAC_1

Proof (of Theorem 2). The security proof differs in Lemmata 21 to 23, 26 and 29 to the single-challenge setting.

The proof uses a hybrid argument with the hybrids G_0 (the $\mathsf{mHPR\text{-}CMA}_{\mathsf{real}}$ game), G_1, $\mathsf{G}_{2,\hat{\imath},0}$, $\mathsf{G}_{2,\hat{\imath},1}$ and $\mathsf{G}_{2,\hat{\imath},3}$–$\mathsf{G}_{2,\hat{\imath},5}$ for $\hat{\imath} \in \{1, \ldots, L\}$, $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},0}$ for $\hat{\imath} \in \{1, \ldots, L\}$ and $\hat{\jmath} \in \{0, \ldots, \hat{\imath}\alpha\}$, $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},1}$–$\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},3}$ for $\hat{\imath} \in \{1, \ldots, L\}$ and $\hat{\jmath} \in \{0, \ldots, \hat{\imath}\alpha - 1\}$ and finally G_3. The hybrids are given in Figure 11 and 12. A summary can be found in Table 4. They make use of random functions $\mathsf{RF}_{\hat{\imath},\hat{\jmath}} : \{0,1\}^{\hat{\jmath}} \to \mathbb{Z}_q^{k\times 2k}$, $\mathsf{ZF}_{\hat{\imath},\hat{\jmath}}, \mathsf{OF}_{\hat{\imath},\hat{\jmath}} : \{0,1\}^{\hat{\jmath}} \to \mathbb{Z}_q^{k\times k}$, defined on-the-fly.

Lemma 15 ($\mathsf{G}_0 \rightsquigarrow \mathsf{G}_1$)**.**

$$\Pr\left[\mathsf{G}_0^{\mathcal{A}} \Rightarrow 1\right] = \Pr\left[\mathsf{G}_1^{\mathcal{A}} \Rightarrow 1\right]$$

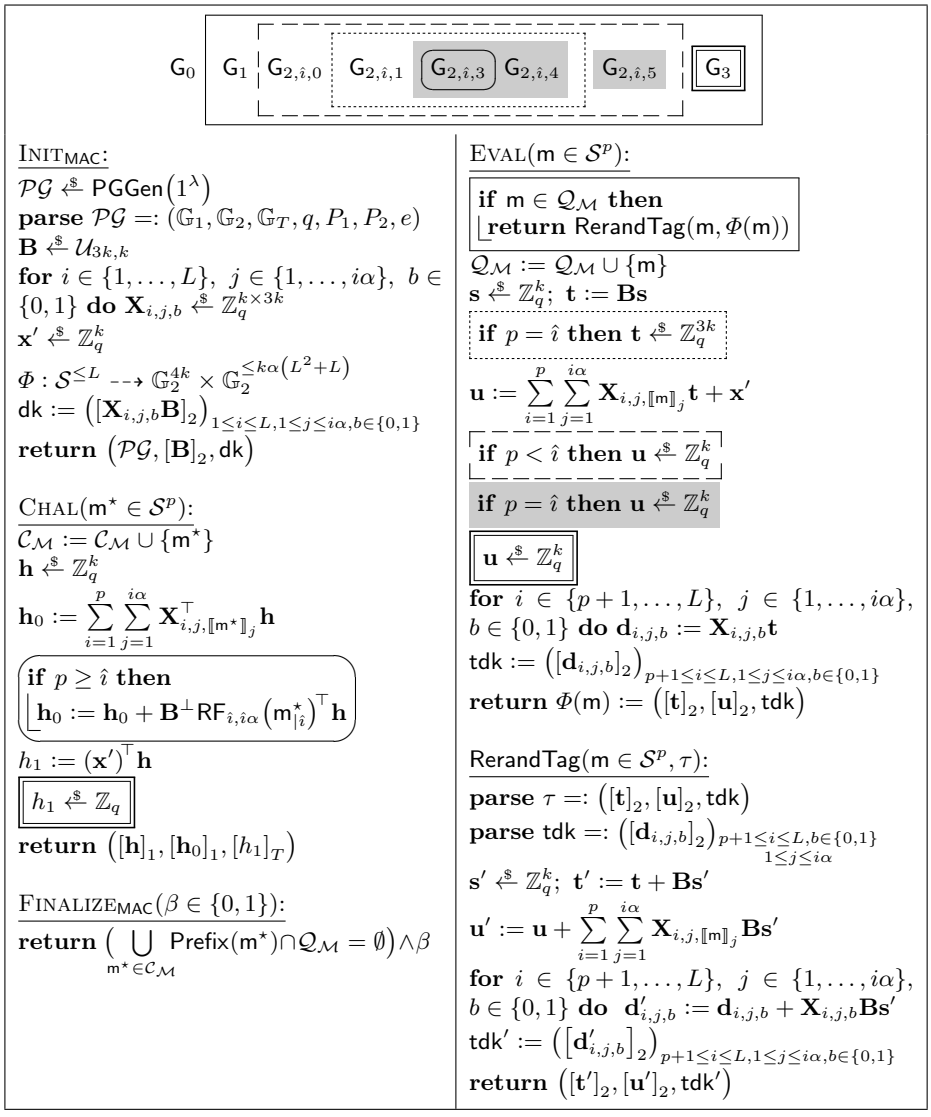


Fig. 11. Hybrids for the mHPR-CMA-security proof of MAC_1. The algorithm RerandTag is only a helper algorithm that rerandomizes tags publicly and not an oracle for the adversary. The partial map Φ is initially totally undefined.

Proof. In game G_1 each time the adversary queries a tag for a message m, where he queried a tag for m before, the adversary will get a rerandomized version of the first tag he queried. The $\mathsf{RerandTag}$ algorithm chooses $\mathbf{t}' := \mathbf{t} + \mathbf{B}\mathbf{s}'$, which is uniformly random in $\mathsf{Span}(\mathbf{B})$ and independent of $\mathbf{t}$, because $\mathbf{s}'$ is uniform random in $\mathbb{Z}_q^k$. The $\mathsf{RerandTag}$ algorithm then computes $\mathbf{u}'$ and a tag delegation key tdk' that forms together with $\mathbf{t}'$ another valid tag for m, that is distributed like a fresh tag, independent of the input tag. Thus the games are equivalent.

Note that the rerandomization uses only the "public key" returned by the INIT oracle so that it could be carried out by the adversary herself. In the following, we will ignore these duplicated EVAL queries. □

Lemma 16 ($\mathsf{G}_1 \rightsquigarrow \mathsf{G}_{2,1,0}$)**.**

$$\Pr\left[\mathsf{G}_1^{\mathcal{A}} \Rightarrow 1\right] = \Pr\left[\mathsf{G}_{2,1,0}^{\mathcal{A}} \Rightarrow 1\right]$$

Proof. These two games are equivalent. □

Lemma 17 ($\mathsf{G}_{2,\hat{\imath},0} \rightsquigarrow \mathsf{G}_{2,\hat{\imath},1}$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}_{2,\hat{\imath},0}^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_{2,\hat{\imath},1}^{\mathcal{A}} \Rightarrow 1\right]\right| \leq 2k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},2}(\mathcal{B}) + \frac{1}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. These two games are equivalent except that in EVAL-queries with $p = \hat{\imath}$ the value $\mathbf{t}$ is chosen uniformly random from $\mathsf{Span}(\mathbf{B})$ in $\mathsf{G}_{2,\hat{\imath},0}$ and uniformly random from $\mathbb{Z}_q^{3k}$ in game $\mathsf{G}_{2,\hat{\imath},1}$. Since for all computed values it is enough to have $[\mathbf{B}]_2$ instead of $\mathbf{B}$, this leads to a straightforward reduction to the Q_e-fold $\mathcal{U}_{3k,k}$-MDDH assumption. By Lemma 3 the Q_e-fold $\mathcal{U}_{3k,k}$-MDDH assumption is at most $2k$ times harder then the $\mathcal{U}_{3k,k}$-MDDH assumption and this assumption is equivalent to the $\mathcal{U}_k$-MDDH assumption by Lemma 1.

The running time of $\mathcal{B}$ is dominated by the running time of $\mathcal{A}$ plus some (polynomial) overhead that is independent of $T(\mathcal{A})$ for the group operations in each oracle query. □

Lemma 18 ($\mathsf{G}_{2,\hat{\imath},1} \rightsquigarrow \mathsf{G}_{2,\hat{\imath},3}$)**.** *For all $\hat{\imath} \in \{1, \ldots, L\}$ and all adversaries $\mathcal{A}$ there exist adversaries $\mathcal{B}_1$, $\mathcal{B}_2$ with*

$$\begin{aligned}|\Pr[\mathsf{G}_{2,\hat{\imath},1} \Rightarrow 1] - \Pr[\mathsf{G}_{2,\hat{\imath},3} \Rightarrow 1]| \leq{}& 8k\hat{\imath}\alpha\left(\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},2}(\mathcal{B}_2)\right) \\ &+ k\hat{\imath}\alpha\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}_1) + \frac{(Q_c+6)\hat{\imath}\alpha}{q-1} + \frac{Q_{e,\hat{\imath}}}{q^{2k}}\end{aligned}$$

and $T(\mathcal{B}_1) \approx T(\mathcal{B}_2) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$. $Q_{e,\hat{\imath}}$ denotes the number of EVAL *queries with $p = \hat{\imath}$.*

Proof. To prove this transition, we use the hybrids $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},0}$ for $\hat{\jmath} \in \{1, \ldots, \hat{\imath}\alpha\}$, $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},1}$–$\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},3}$ for $\hat{\jmath} \in \{1, \ldots, \hat{\imath}\alpha - 1\}$. The hybrids are given in Figure 12.

Lemma 18 follows directly from Lemmata 19–25. □

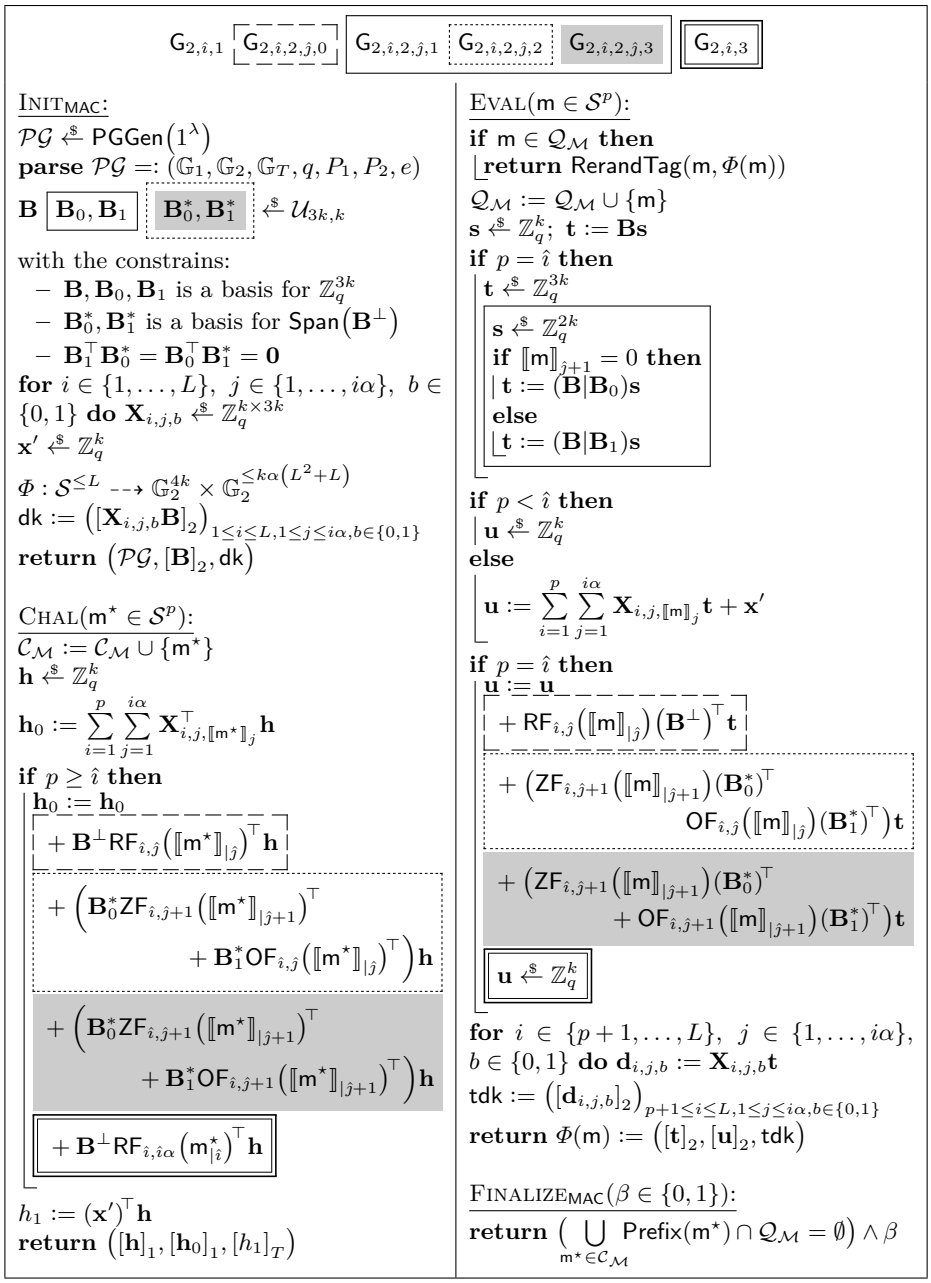


Fig. 12. Hybrids for the transition from $\mathsf{G}_{2,\hat{\imath},1}$ to $\mathsf{G}_{2,\hat{\imath},3}$. The helper algorithm $\mathsf{RerandTag}$ that rerandomizes tags publicly is defined in Figure 11.

Lemma 19 ($\mathsf{G}_{2,\hat{\imath},1} \rightsquigarrow \mathsf{G}_{2,\hat{\imath},2,0,0}$)**.**

$$\Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},1} \Rightarrow 1\right] = \Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},2,0,0} \Rightarrow 1\right]$$

Proof. These two games are equivalent. When replacing in $\mathsf{G}_{2,\hat{\imath},1}$ the secret values $\mathbf{X}_{\hat{\imath},1,b}$ with $\mathbf{X}_{\hat{\imath},1,b} + \mathsf{RF}_{\hat{\imath},0}(\varepsilon)\left(\mathbf{B}^{\perp}\right)^{\top}$ (for $b \in \{0,1\}$), we get game $\mathsf{G}_{2,\hat{\imath},2,0,0}$. The distribution of $\mathbf{X}_{\hat{\imath},1,b}$ and $\mathbf{X}_{\hat{\imath},1,b} + \mathsf{RF}_{\hat{\imath},0}(\varepsilon)\left(\mathbf{B}^{\perp}\right)^{\top}$ is identical. Note that the term $\mathsf{RF}_{\hat{\imath},0}(\varepsilon)\left(\mathbf{B}^{\perp}\right)^{\top}$ cancels out in the master public key and in the user delegation keys of EVAL-queries with $p < \hat{\imath}$. □

Lemma 20 ($\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},0} \rightsquigarrow \mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},1}$)**.** *For all $\hat{\jmath} < \hat{\imath}\alpha$ adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},2,\hat{\jmath},0} \Rightarrow 1\right] - \Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},2,\hat{\jmath},1} \Rightarrow 1\right]\right| \leq 4k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},2}(\mathcal{B}) + \frac{2}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. These two games are equivalent except that in the EVAL queries the vector $\mathbf{t}$ is generated uniformly random from $\mathbb{Z}_q^{3k}$ in game $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},0}$ and from either $\mathsf{Span}(\mathbf{B}|\mathbf{B}_0)$ or $\mathsf{Span}(\mathbf{B}|\mathbf{B}_1)$ depending on the bit $[\![\mathsf{m}]\!]_{\hat{\jmath}+1}$ in game $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},1}$. We can switch from $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},0}$ to $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},1}$ with two Q_e-fold $\mathcal{U}_{3k,k}$-MDDH challenges.

To achieve that, we first switch $\mathbf{t}$ in EVAL queries with $[\![\mathsf{m}]\!]_{\hat{\jmath}+1} = 0$ from a random vector in $\mathbb{Z}_q^{3k}$ to $\mathbf{t} := \mathbf{B}\mathbf{s}_1 + \mathbf{s}_2$ where $\mathbf{s}_1 \xleftarrow{\$} \mathbb{Z}_q^k$ and $\mathbf{s}_2 \xleftarrow{\$} \mathbb{Z}_q^{3k}$. This change is only conceptual. Then we change $\mathbf{s}_2$ from a random vector in $\mathbb{Z}_q^{3k}$ to a random vector in the span of $\mathbf{B}_0$ with a Q_e-fold $\mathcal{U}_{3k,k}$-MDDH challenge.

To ensure that the column vectors of $(\mathbf{B}|\mathbf{B}_0|\mathbf{B}_1)$ form a basis of $\mathbb{Z}_q^{3k}$, the reduction chooses $\mathbf{B}, \mathbf{B}_1 \xleftarrow{\$} \mathcal{U}_{3k,k}$ such that $(\mathbf{B}|\mathbf{B}_1)$ has rank $2k$ and checks whether the kernels of $\mathbf{B}_0^{\top}$ and $(\mathbf{B}|\mathbf{B}_1)^{\top}$ are disjoint. This is equivalent to $(\mathbf{B}|\mathbf{B}_0|\mathbf{B}_1)$ forming a basis of $\mathbb{Z}_q^{3k}$ and can be done over the group by testing for all column vectors $\mathbf{b}$ of $(\mathbf{B}|\mathbf{B}_1)^{\perp}$ whether $\mathbf{B}_0^{\top}\mathbf{b} \neq \mathbf{0}$. By generating new matrices $\mathbf{B}, \mathbf{B}_1 \xleftarrow{\$} \mathcal{U}_{3k,k}$ until this is satisfied, we can ensure that $\mathbf{B}, \mathbf{B}_0, \mathbf{B}_1$ is a basis of $\mathbb{Z}_q^{3k}$.

With the same argument, we can switch $\mathbf{t}$ from a random vector in $\mathbb{Z}_q^{3k}$ to a random vector in $\mathsf{Span}(\mathbf{B}|\mathbf{B}_1)$ in EVAL queries with $[\![\mathsf{m}]\!]_{\hat{\jmath}+1} = 1$.

The running time of $\mathcal{B}$ is dominated by the running time of $\mathcal{A}$ plus some (polynomial) overhead that is independent of $T(\mathcal{A})$ for the group operations in each oracle query. □

Lemma 21 ($\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},1} \rightsquigarrow \mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},2}$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},2,\hat{\jmath},1} \Rightarrow 1\right] - \Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},2,\hat{\jmath},2} \Rightarrow 1\right]\right| \leq k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}) + \frac{Q_c + 2}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. First of all, we replace in game $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},1}$ the term $\mathsf{RF}_{\hat{\imath},\hat{\jmath}}\left(\llbracket\mathsf{m}\rrbracket_{|\hat{\jmath}}\right)\left(\mathbf{B}^{\perp}\right)^{\top}$ with $\mathsf{ZF}_{\hat{\imath},\hat{\jmath}}\left(\llbracket\mathsf{m}\rrbracket_{|\hat{\jmath}}\right)\left(\mathbf{B}_0^*\right)^{\top} + \mathsf{OF}_{\hat{\imath},\hat{\jmath}}\left(\llbracket\mathsf{m}\rrbracket_{|\hat{\jmath}}\right)\left(\mathbf{B}_1^*\right)^{\top}$. This does not change the distribution, since $\mathbf{B}_0, \mathbf{B}_1$ is a basis for $\mathsf{Span}\left(\mathbf{B}^{\perp}\right)$.

We define

$$\mathsf{ZF}_{\hat{\imath},\hat{\jmath}+1}\left(\llbracket\mathsf{m}\rrbracket_{|\hat{\jmath}+1}\right) := \begin{cases} \mathsf{ZF}_{\hat{\imath},\hat{\jmath}}\left(\llbracket\mathsf{m}\rrbracket_{|\hat{\jmath}}\right) & \text{if } \llbracket\mathsf{m}\rrbracket_{\hat{\jmath}+1} = 0 \\ \mathsf{ZF}_{\hat{\imath},\hat{\jmath}}\left(\llbracket\mathsf{m}\rrbracket_{|\hat{\jmath}}\right) + \mathsf{ZF}'_{\hat{\imath},\hat{\jmath}}\left(\llbracket\mathsf{m}\rrbracket_{|\hat{\jmath}}\right) & \text{if } \llbracket\mathsf{m}\rrbracket_{\hat{\jmath}+1} = 1 \end{cases},$$

where $\mathsf{ZF}'_{\hat{\imath},\hat{\jmath}} : \{0,1\}^{\hat{\jmath}} \to \mathbb{Z}_q^{k\times k}$ is another independent random function. Since $\mathsf{ZF}_{\hat{\imath},\hat{\jmath}}$ does not appear in game $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},2}$ anymore, $\mathsf{ZF}_{\hat{\imath},\hat{\jmath}+1}$ is a random function.

Take a kQ_c-fold $\mathcal{U}_{2k,k}$-MDDH challenge $\left([\mathbf{D}]_1, [\mathbf{f}_1]_1, \ldots, [\mathbf{f}_{kQ_c}]_1\right)$ and define $\mathbf{F}_c := \left(\mathbf{f}_{(c-1)k+1} | \ldots | \mathbf{f}_{ck}\right)$ to get Q_c $2k \times k$ matrices, whose column vectors are uniformly random chosen from either $\mathsf{Span}(\mathbf{D})$ or $\mathbb{Z}_q^{2k}$. Then the reduction in Figure 13 can be used to bound the difference between $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},1}$ and $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},2}$.

Eval queries with $p \neq \hat{\imath}$ use the same code in both games and in the reduction. Eval queries with $p = \hat{\imath}$ and $\llbracket\mathsf{m}\rrbracket_{\hat{\jmath}+1} = 0$ are distributed identically in both games, by definition of $\mathsf{RF}^{(0)}_{\hat{\imath},\hat{\jmath}+1}$. They are simulated correctly in the reduction since $\mathbf{X}_{\hat{\imath},\hat{\jmath}+1,1}$ is not used to answer those queries.

Eval queries with $p = \hat{\imath}$ and $\llbracket\mathsf{m}\rrbracket_{\hat{\jmath}+1} = 1$ are distributed identically in both games, since for those queries $\mathbf{t} \in \mathsf{Span}(\mathbf{B}|\mathbf{B}_1)$ and both $\mathbf{B}$ and $\mathbf{B}_1$ are orthogonal to $\mathbf{B}_0^*$. Thus $\mathsf{ZF}_{\hat{\imath},\hat{\jmath}+1}\left(\llbracket\mathsf{m}\rrbracket_{|\hat{\jmath}+1}\right)\left(\mathbf{B}_0^*\right)^{\top}\mathbf{t} = 0$. They are simulated correctly in the reduction because $\mathbf{X}_{\hat{\imath},\hat{\jmath}+1,1}\mathbf{t} = \mathbf{J}_{\hat{\imath},\hat{\jmath}+1,1}\mathbf{t}$.

Assume that $\overline{\mathbf{D}}$ is invertible. This happens with probability at least $(1 - 1/(q-1))$. To analyze the Chal queries define $\mathbf{F}_c =: \begin{pmatrix} \overline{\mathbf{D}}\mathbf{W}_c \\ \underline{\mathbf{D}}\mathbf{W}_c + \mathbf{R}_c \end{pmatrix}$ where $\mathbf{W}_c$ is uniform random in $\mathbb{Z}_q^{k\times k}$ and $\mathbf{R}_c$ is $\mathbf{0} \in \mathbb{Z}_q^{k\times k}$ or uniform random in $\mathbb{Z}_q^{k\times k}$. Assume in the following that $\mathbf{W}_c$ has full rank. This happens with probability at least $(1 - 1/(q-1))$. The reduction uses in Chal queries $\mathbf{h} := \overline{\mathbf{F}_c}\mathbf{h}'$. Since $\overline{\mathbf{F}_c}$ has full rank and $\mathbf{h}'$ is uniformly random in $\mathbb{Z}_q^k$, $\mathbf{h}$ is distributed correctly.

Chal queries with $p < \hat{\imath}$ or $\llbracket\mathsf{m}^\star\rrbracket_{\hat{\jmath}+1} = 0$ are distributed identically in both games. They are simulated correctly by the reduction because $\mathbf{X}_{\hat{\imath},\hat{\jmath}+1,1}$ is not used to answer those queries.

The reduction computes in Chal queries with $p \geq \hat{\imath}$ and $\llbracket\mathsf{m}^\star\rrbracket_{\hat{\jmath}+1} = 1$ $\mathbf{h}_0$ as

$$\begin{aligned}
\mathbf{h}_0 &:= \left(\sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{J}^{\top}_{i,j,\llbracket\mathsf{m}^\star\rrbracket_j} + \mathsf{F}\left(\llbracket\mathsf{m}^\star\rrbracket_{|\hat{\jmath}}\right)\right)\mathbf{h} + \mathbf{B}_0^*\underline{\mathbf{F}_c}\mathbf{h}' \\
&= \left(\sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{J}^{\top}_{i,j,\llbracket\mathsf{m}^\star\rrbracket_j} + \mathsf{F}\left(\llbracket\mathsf{m}^\star\rrbracket_{|\hat{\jmath}}\right)\right)\mathbf{h} + \mathbf{B}_0^*\underline{\mathbf{D}}\overline{\mathbf{D}}^{-1}\mathbf{h}\overline{\mathbf{F}_c}\mathbf{h}' + \mathbf{B}_0^*\mathbf{R}_c\mathbf{h}' \\
&= \left(\sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{X}^{\top}_{i,j,\llbracket\mathsf{m}^\star\rrbracket_j} + \mathsf{F}\left(\llbracket\mathsf{m}^\star\rrbracket_{|\hat{\jmath}}\right)\right)\mathbf{h} + \mathbf{B}_0^*\mathbf{R}_c\overline{\mathbf{F}_c}^{-1}\mathbf{h}\,.
\end{aligned}$$

$\underline{\text{INIT}_{\mathsf{MAC}}}$:
parse $\mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
$\mathbf{B}, \mathbf{B}_0, \mathbf{B}_1, \mathbf{B}_0^*, \mathbf{B}_1^* \xleftarrow{\$} \mathcal{U}_{3k,k}$
with the constrains:
- $\mathbf{B}, \mathbf{B}_0, \mathbf{B}_1$ is a basis for $\mathbb{Z}_q^{3k}$
- $\mathbf{B}_0^*, \mathbf{B}_1^*$ is a basis for $\mathsf{Span}\big(\mathbf{B}^\perp\big)$
- $\mathbf{B}_1^\top \mathbf{B}_0^* = \mathbf{B}_0^\top \mathbf{B}_1^* = \mathbf{0}$

for $i \in \{1, \dots, L\},\ j \in \{1, \dots, i\alpha\},\ b \in \{0,1\}$ **do**
  $\mathbf{J}_{i,j,b} \xleftarrow{\$} \mathbb{Z}_q^{k \times 3k}$
  if $(i,j,b) \neq (\hat{\imath}, \hat{\jmath}+1, 1)$ **then**
    $\underline{\mathbf{X}}_{i,j,b} := \mathbf{J}_{i,j,b}$
// Implicit:
// $\mathbf{X}_{\hat{\imath},\hat{\jmath}+1,1} := \mathbf{J}_{\hat{\imath},\hat{\jmath}+1,1} + \overline{\mathbf{D}}^{-\top} \underline{\mathbf{D}}^\top (\mathbf{B}_0^*)^\top$
$\mathbf{x}' \xleftarrow{\$} \mathbb{Z}_q^k$
$\Phi : \mathcal{S}^{\le L} \dashrightarrow \mathbb{G}_2^{4k} \times \mathbb{G}_2^{\le k\alpha(L^2+L)}$
$\mathsf{dk} := \big([\mathbf{J}_{i,j,b}\mathbf{B}]_2\big)_{1 \le i \le L, 1 \le j \le i\alpha, b \in \{0,1\}}$
return $\big(\mathcal{PG}, [\mathbf{B}]_2, \mathsf{dk}\big)$

$\underline{\text{CHAL}(\mathsf{m}^\star \in \mathcal{S}^p)}$:
$\mathcal{C}_\mathcal{M} := \mathcal{C}_\mathcal{M} \cup \{\mathsf{m}^\star\}$
Let c be the index of the first CHAL query on a message with prefix $[\![\mathsf{m}^\star]\!]_{|\hat{\jmath}}$.
$\mathbf{h}' \xleftarrow{\$} \mathbb{Z}_q^k$
$\mathbf{h} := \overline{\mathbf{F}}_c \mathbf{h}'$
$\mathbf{h}_0 := \sum_{i=1}^{p} \sum_{j=1}^{i\alpha} \mathbf{J}_{i,j,[\![\mathsf{m}^\star]\!]_j}^\top \mathbf{h}$
if $p \ge \hat{\imath}$ **then**
  $\mathbf{h}_0 := \mathbf{h}_0 + \Big(\mathbf{B}_0^* \mathsf{ZF}_{\hat{\imath},\hat{\jmath}}\big([\![\mathsf{m}^\star]\!]_{|\hat{\jmath}}\big)^\top + \mathbf{B}_1^* \mathsf{OF}_{\hat{\imath},\hat{\jmath}}\big([\![\mathsf{m}^\star]\!]_{|\hat{\jmath}}\big)^\top\Big)\mathbf{h}$
  if $[\![\mathsf{m}^\star]\!]_{\hat{\jmath}+1} = 1$ **then**
    $\mathbf{h}_0 := \mathbf{h}_0 + \mathbf{B}_0^* \underline{\mathbf{F}_c} \mathbf{h}'$
$h_1 := (\mathbf{x}')^\top \mathbf{h}$
return $\big([\mathbf{h}]_1, [\mathbf{h}_0]_1, [h_1]_T\big)$

$\underline{\text{EVAL}(\mathsf{m} \in \mathcal{S}^p)}$:
if $\mathsf{m} \in \mathcal{Q}_\mathcal{M}$ **then**
  return $\mathsf{RerandTag}(\mathsf{m}, \Phi(\mathsf{m}))$
$\mathcal{Q}_\mathcal{M} := \mathcal{Q}_\mathcal{M} \cup \{\mathsf{m}\}$
$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k;\ \mathbf{t} := \mathbf{B}\mathbf{s}$
if $p = \hat{\imath}$ **then**
  $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^{2k}$
  if $[\![\mathsf{m}]\!]_{\hat{\jmath}+1} = 0$ **then**
    $\mathbf{t} := (\mathbf{B}|\mathbf{B}_0)\mathbf{s}$
  else
    $\mathbf{t} := (\mathbf{B}|\mathbf{B}_1)\mathbf{s}$
if $p < \hat{\imath}$ **then**
  $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^k$
else
  $\mathbf{u} := \sum_{i=1}^{p} \sum_{j=1}^{i\alpha} \mathbf{J}_{i,j,[\![\mathsf{m}]\!]_j} \mathbf{t} + \mathbf{x}'$
if $p = \hat{\imath}$ **then**
  $\mathbf{u} := \mathbf{u} + \Big(\mathsf{ZF}_{\hat{\imath},\hat{\jmath}}\big([\![\mathsf{m}]\!]_{|\hat{\jmath}}\big)(\mathbf{B}_0^*)^\top + \mathsf{OF}_{\hat{\imath},\hat{\jmath}}\big([\![\mathsf{m}]\!]_{|\hat{\jmath}}\big)(\mathbf{B}_1^*)^\top\Big)\mathbf{t}$
for $i \in \{p+1, \dots, L\},\ j \in \{1, \dots, i\alpha\},\ b \in \{0,1\}$ **do** $\mathbf{d}_{i,j,b} := \mathbf{J}_{i,j,b}\mathbf{t}$
$\mathsf{tdk} := \big([\mathbf{d}_{i,j,b}]_2\big)_{p+1 \le i \le L, 1 \le j \le i\alpha, b \in \{0,1\}}$
return $\Phi(\mathsf{m}) := \big([\mathbf{t}]_2, [\mathbf{u}]_2, \mathsf{tdk}\big)$

$\underline{\text{FINALIZE}_{\mathsf{MAC}}(\beta \in \{0,1\})}$:
return $\Big(\bigcup_{\mathsf{m}^\star \in \mathcal{C}_\mathcal{M}} \mathsf{Prefix}(\mathsf{m}^\star) \cap \mathcal{Q}_\mathcal{M} = \emptyset\Big) \wedge \beta$

Fig. 13. Reduction for the transition from $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},1}$ to $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},2}$ to the kQ_c-fold $\mathcal{U}_{2k,k}$-MDDH challenge $\big([\mathbf{D}]_1, [\mathbf{F}_1]_1, \dots, [\mathbf{F}_{Q_c}]_1\big)$.

with

$$\mathsf{F}\left(\llbracket \mathsf{m}^\star \rrbracket_{|\hat{\jmath}}\right) := \mathbf{B}_0^* \mathsf{ZF}_{\hat{\imath},\hat{\jmath}}\left(\llbracket \mathsf{m}^\star \rrbracket_{|\hat{\jmath}}\right)^\top + \mathbf{B}_1^* \mathsf{OF}_{\hat{\imath},\hat{\jmath}}\left(\llbracket \mathsf{m}^\star \rrbracket_{|\hat{\jmath}}\right)^\top.$$

If $\mathbf{R}_c = \mathbf{0}$, the reduction is simulating $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},1}$. If $\mathbf{R}_c$ is uniformly random, we implicitly set $\mathsf{ZF}'_{\hat{\imath},\hat{\jmath}}\left(\llbracket \mathsf{m}^\star \rrbracket_{|\hat{\jmath}}\right)^\top := \mathbf{R}_c \overline{\mathbf{F}_c}^{-1}$ and are simulating game $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},2}$. □

Lemma 22 ($\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},2} \rightsquigarrow \mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},3}$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},2,\hat{\jmath},2} \Rightarrow 1\right] - \Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},2,\hat{\jmath},3} \Rightarrow 1\right]\right| \leq k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}) + \frac{Q_c + 2}{q - 1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. We define

$$\mathsf{OF}_{\hat{\imath},\hat{\jmath}+1}\left(\llbracket \mathsf{m} \rrbracket_{|\hat{\jmath}+1}\right) := \begin{cases} \mathsf{OF}_{\hat{\imath},\hat{\jmath}}\left(\llbracket \mathsf{m} \rrbracket_{|\hat{\jmath}}\right) + \mathsf{OF}'_{\hat{\imath},\hat{\jmath}}\left(\llbracket \mathsf{m} \rrbracket_{|\hat{\jmath}}\right) & \text{if } \llbracket \mathsf{m} \rrbracket_{\hat{\jmath}+1} = 0 \\ \mathsf{OF}_{\hat{\imath},\hat{\jmath}}\left(\llbracket \mathsf{m} \rrbracket_{|\hat{\jmath}}\right) & \text{if } \llbracket \mathsf{m} \rrbracket_{\hat{\jmath}+1} = 1 \end{cases},$$

where $\mathsf{OF}'_{\hat{\imath},\hat{\jmath}} : \{0,1\}^{\hat{\jmath}} \to \mathbb{Z}_q^{k \times k}$ is another independent random function. Since $\mathsf{OF}_{\hat{\imath},\hat{\jmath}}$ does not appear in game $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},3}$ anymore, $\mathsf{OF}_{\hat{\imath},\hat{\jmath}+1}$ is a random function.

The proof for this Lemma is analogous to the proof of Lemma 21, just with the roles of 0 and 1 swapped. □

Lemma 23 (Optimization: $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},1} \rightsquigarrow \mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},3}$**).** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},2,\hat{\jmath},1} \Rightarrow 1\right] - \Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},2,\hat{\jmath},3} \Rightarrow 1\right]\right| \leq k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}) + \frac{Q_c + 2}{q - 1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. We can do the reduction of Lemmata 21 and 22 in one step using only one MDDH challenge in $\mathbb{G}_1$. This combined reduction embeds the challenge in both $\mathbf{X}_{\hat{\imath},\hat{\jmath}+1,1}$ as $\mathbf{X}_{\hat{\imath},\hat{\jmath}+1,1} := \mathbf{J}_{\hat{\imath},\hat{\jmath}+1,1} + \mathbf{B}_0^* \underline{\mathbf{D}} \overline{\mathbf{D}}^{-1}$ and $\mathbf{X}_{\hat{\imath},\hat{\jmath}+1,0}$ as $\mathbf{X}_{\hat{\imath},\hat{\jmath}+1,0} := \mathbf{J}_{\hat{\imath},\hat{\jmath}+1,0} + \mathbf{B}_1^* \underline{\mathbf{D}} \overline{\mathbf{D}}^{-1}$ and picks in each CHAL query on $\mathsf{m}^\star$ c as the index of the first CHAL query on a message with prefix $\llbracket \mathsf{m}^\star \rrbracket_{|\hat{\jmath}+1}$. □

Lemma 24 ($\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},3} \rightsquigarrow \mathsf{G}_{2,\hat{\imath},2,\hat{\jmath}+1,0}$)**.** *For $\hat{\jmath} < \hat{\imath}\alpha$ and all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},2,\hat{\jmath},3} \Rightarrow 1\right] - \Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},2,\hat{\jmath}+1,0} \Rightarrow 1\right]\right| \leq 4k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},2}(\mathcal{B}) + \frac{2}{q - 1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. First of all, we replace in game $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},3}$ the term $\mathsf{ZF}_{\hat{\imath},\hat{\jmath}+1}\Big(\llbracket \mathsf{m} \rrbracket_{|\hat{\jmath}+1}\Big)(\mathbf{B}_0^*)^\top + \mathsf{OF}_{\hat{\imath},\hat{\jmath}+1}\Big(\llbracket \mathsf{m} \rrbracket_{|\hat{\jmath}+1}\Big)(\mathbf{B}_1^*)^\top$ with $\mathsf{RF}_{\hat{\imath},\hat{\jmath}+1}\Big(\llbracket \mathsf{m} \rrbracket_{|\hat{\jmath}+1}\Big)\big(\mathbf{B}^\perp\big)^\top$ to avoid computing $\mathbf{B}_0^*$ and $\mathbf{B}_1^*$. This does not change the distribution, since $\mathbf{B}_0^*, \mathbf{B}_1^*$ is a basis for $\mathsf{Span}\big(\mathbf{B}^\perp\big)$. It remains to switch the distribution from $\mathbf{t}$ back to uniform random using two Q_e-fold $\mathcal{U}_{3k,k}$-MDDH challenges. This part is the reverse of Lemma 20. □

Lemma 25 ($\mathsf{G}_{2,\hat{\imath},2,\hat{\imath}\alpha,0} \rightsquigarrow \mathsf{G}_{2,\hat{\imath},3}$)**.** *Let $Q_{e,\hat{\imath}}$ denote the number of* Eval *queries with $p = \hat{\imath}$.*

$$\big|\Pr\big[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},2,\hat{\imath}\alpha,0} \Rightarrow 1\big] - \Pr\big[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},3} \Rightarrow 1\big]\big| \leq \frac{Q_{e,\hat{\imath}}}{q^{2k}}$$

Proof. Assume $\forall \mathsf{m}^\star \in \mathcal{C}_{\mathcal{M}} : \mathsf{Prefix}(\mathsf{m}^\star) \cap \mathcal{Q}_{\mathcal{M}} \neq \emptyset$, otherwise the adversary has lost the game anyway. In each user secret key query with $p = \hat{\imath}$ the value $\mathsf{RF}_{\hat{\imath},\hat{\imath}\alpha}(\mathsf{m})\big(\mathbf{B}^\perp\big)^\top\mathbf{t}$ is added to $\mathbf{u}$. This is the only place where $\mathsf{RF}_{\hat{\imath},\hat{\imath}\alpha}(\mathsf{m})$ is used, since only the first Eval query for each message evaluates the random function and Chal queries evaluate $\mathsf{RF}_{\hat{\imath},\hat{\imath}\alpha}$ only on prefixes of $\mathsf{m}^\star \in \mathcal{C}_{\mathcal{M}}$. Thus each non-duplicated Eval query outputs a uniformly random vector for $\mathbf{u}$ when $\mathbf{t} \notin \mathsf{Span}(\mathbf{B})$, which happens with probability at least $(1 - 1/\big(q^{2k}\big))$. In this case the games are distributed identically. □

Lemma 26 ($\mathsf{G}_{2,\hat{\imath},3} \rightsquigarrow \mathsf{G}_{2,\hat{\imath},4}$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\big|\Pr\big[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},3} \Rightarrow 1\big] - \Pr\big[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},4} \Rightarrow 1\big]\big| \leq 2k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}) + \frac{Q_c + 2}{q - 1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. In $\mathsf{G}_{2,\hat{\imath},4}$ we remove the random function term from $\mathbf{h}_0$ compared to $\mathsf{G}_{2,\hat{\imath},3}$. This step is necessary to avoid having to compute $\mathbf{B}^\perp$ and thus being able to perform MDDH challenges on $\mathbf{B}$.

To bound the difference between these two games, we need a kQ_c-fold $\mathcal{U}_{3k,k}$-MDDH challenge $\big([\mathbf{D}]_1, [\mathbf{f}_1]_1, \ldots, [\mathbf{f}_{kQ_c}]_1\big)$ and group the kQ_c vectors $[\mathbf{f}_1]_1, \ldots$ $\ldots, [\mathbf{f}_{kQ_c}]_1$ to Q_c $3k \times k$ matrices $[\mathbf{F}_1]_1, \ldots, [\mathbf{F}_{kQ_c}]_1$. Then use the reduction given in Figure 14.

The reduction correctly simulates the Init oracle and Eval queries with $p \neq \hat{\imath}$ because the $\mathbf{B}^\perp$ part of $\mathbf{X}_{\hat{\imath},1,b}$ cancels out there. Eval queries with $p = \hat{\imath}$ are also simulated correctly because they pick $\mathbf{u}$ uniformly random and do not use $\mathbf{X}_{\hat{\imath},1,b}$.

Assume that $\overline{\mathbf{D}}$ is invertible. This happens with probability at least $(1 - 1/(q-1))$. To analyze the Chal queries define $\mathbf{F}_c =: \begin{pmatrix} \overline{\mathbf{D}}\mathbf{W}_c \\ \underline{\mathbf{D}}\mathbf{W}_c + \mathbf{R}_c \end{pmatrix}$ where $\mathbf{W}_c$ is uniform random in $\mathbb{Z}_q^{k\times k}$ and $\mathbf{R}_c$ is $\mathbf{0} \in \mathbb{Z}_q^{2k\times k}$ or uniform random in $\mathbb{Z}_q^{2k\times k}$. Assume that $\mathbf{W}_c$ has full rank. This happens with probability at least $(1 - 1/(q-1))$. The reduction uses in Chal queries $\mathbf{h} := \overline{\mathbf{F}_c}\mathbf{h}'$. This is correctly distributed since $\overline{\mathbf{F}_c}$ has full rank and $\mathbf{h}'$ is uniformly random in $\mathbb{Z}_q^k$.

$\underline{\text{INIT}_{\mathsf{MAC}}}$:
parse $\mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
$\mathbf{B} \xleftarrow{\$} \mathcal{U}_{3k,k}$
for $i \in \{1, \dots, L\},\ j \in \{1, \dots, i\alpha\},\ b \in \{0,1\}$ **do**
  $\mathbf{J}_{i,j,b} \xleftarrow{\$} \mathbb{Z}_q^{k \times 3k}$
  if $(i,j) \neq (\hat{\imath}, 1)$ **then** $\mathbf{X}_{i,j,b} := \mathbf{J}_{i,j,b}$
// Implicit: For $b \in \{0,1\}$:
// $\mathbf{X}_{\hat{\imath},1,b} := \mathbf{J}_{\hat{\imath},1,b} + \overline{\mathbf{D}}^{-\top} \underline{\mathbf{D}}^{\top} \mathbf{B}^{\perp}$
$\mathbf{x}' \xleftarrow{\$} \mathbb{Z}_q^k$
$\Phi : \mathcal{S}^{\leq L} \dashrightarrow \mathbb{G}_2^{4k} \times \mathbb{G}_2^{\leq k\alpha\left(L^2+L\right)}$
$\mathsf{dk} := \left([\mathbf{J}_{i,j,b}\mathbf{B}]_2\right)_{1 \leq i \leq L, 1 \leq j \leq i\alpha, b \in \{0,1\}}$
return $\left(\mathcal{PG}, [\mathbf{B}]_2, \mathsf{dk}\right)$

$\underline{\text{FINALIZE}_{\mathsf{MAC}}(\beta \in \{0,1\})}$:
return $\left(\bigcup_{\mathsf{m}^\star \in \mathcal{C}_{\mathcal{M}}} \mathsf{Prefix}(\mathsf{m}^\star) \cap \mathcal{Q}_{\mathcal{M}} = \emptyset\right) \wedge \beta$

$\underline{\text{EVAL}(\mathsf{m} \in \mathcal{S}^p)}$:
if $\mathsf{m} \in \mathcal{Q}_{\mathcal{M}}$ **then**
  return $\mathsf{RerandTag}(\mathsf{m}, \Phi(\mathsf{m}))$
$\mathcal{Q}_{\mathcal{M}} := \mathcal{Q}_{\mathcal{M}} \cup \{\mathsf{m}\}$
$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k;\ \mathbf{t} := \mathbf{Bs}$
if $p = \hat{\imath}$ **then** $\mathbf{t} \xleftarrow{\$} \mathbb{Z}_q^{3k}$
$\mathbf{u} := \sum_{i=1}^{p} \sum_{j=1}^{i\alpha} \mathbf{J}_{i,j,[\![\mathsf{m}]\!]_j} \mathbf{t} + \mathbf{x}'$
if $p \leq \hat{\imath}$ **then** $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^k$
for $i \in \{p+1, \dots, L\},\ j \in \{1, \dots, i\alpha\},\ b \in \{0,1\}$ **do** $\mathbf{d}_{i,j,b} := \mathbf{J}_{i,j,b}\mathbf{t}$
$\mathsf{tdk} := \left([\mathbf{d}_{i,j,b}]_2\right)_{p+1 \leq i \leq L, 1 \leq j \leq i\alpha, b \in \{0,1\}}$
return $\Phi(\mathsf{m}) := \left([\mathbf{t}]_2, [\mathbf{u}]_2, \mathsf{tdk}\right)$

$\underline{\text{CHAL}(\mathsf{m}^\star \in \mathcal{S}^p)}$:
$\mathcal{C}_{\mathcal{M}} := \mathcal{C}_{\mathcal{M}} \cup \{\mathsf{m}^\star\}$
Let c be the index of the first CHAL query on a message with prefix $\mathsf{m}^\star_{|\hat{\imath}}$.
$\mathbf{h}' \xleftarrow{\$} \mathbb{Z}_q^k$
$\mathbf{h} := \overline{\mathbf{F}_c}\mathbf{h}'$
$\mathbf{h}_0 := \sum_{i=1}^{p} \sum_{j=1}^{i\alpha} \mathbf{J}_{i,j,[\![\mathsf{m}^\star]\!]_j}^{\top} \mathbf{h}$
if $p \geq \hat{\imath}$ **then** $\mathbf{h}_0 := \mathbf{h}_0 + \mathbf{B}^{\perp} \underline{\mathbf{F}_c} \mathbf{h}'$
$h_1 := (\mathbf{x}')^{\top} \mathbf{h}$
return $\left([\mathbf{h}]_1, [\mathbf{h}_0]_1, [h_1]_T\right)$

Fig. 14. Reduction for the transition from $\mathsf{G}_{2,\hat{\imath},3}$ to $\mathsf{G}_{2,\hat{\imath},4}$ to the kQ_c-fold $\mathcal{U}_{2k,k}$-MDDH challenge $\left([\mathbf{D}]_1, [\mathbf{F}_1]_1, \dots, [\mathbf{F}_{Q_c}]_1\right)$.

The reduction computes in CHAL queries with $p \geq \hat{\imath}$ $\mathbf{h}_0$ as

$$\begin{aligned}\mathbf{h}_0 &:= \sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{J}_{i,j,[\![\mathsf{m}^\star]\!]_j}^\top \mathbf{h} + \mathbf{B}^\perp \underline{\mathbf{F}_c}\mathbf{h}' \\ &= \sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{J}_{i,j,[\![\mathsf{m}^\star]\!]_j}^\top \mathbf{h} + \mathbf{B}^\perp \underline{\mathbf{D}}\overline{\mathbf{D}}^{-1}\overline{\mathbf{F}_c}\mathbf{h}' + \mathbf{B}^\perp \mathbf{R}_c\mathbf{h}' \\ &= \sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{X}_{i,j,[\![\mathsf{m}^\star]\!]_j}^\top \mathbf{h} + \mathbf{B}^\perp \mathbf{R}_c\overline{\mathbf{F}_c}^{-1}\mathbf{h}\,.\end{aligned}$$

If $\mathbf{R}_c$ is uniformly random implicitly set $\mathsf{RF}_{\hat{\imath},\hat{\imath}\alpha}\left(\mathsf{m}^\star_{|\hat{\imath}}\right)^\top := \mathbf{R}_c\overline{\mathbf{F}_c}^{-1}$ and the reduction is simulating game $\mathsf{G}_{2,\hat{\imath},3}$. If $\mathbf{R}_c = 0$ the reduction is simulating game $\mathsf{G}_{2,\hat{\imath},4}$. □

Lemma 27 ($\mathsf{G}_{2,\hat{\imath},4} \rightsquigarrow \mathsf{G}_{2,\hat{\imath},5}$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},4} \Rightarrow 1\right] - \Pr[\mathsf{G}_{2,\hat{\imath},5} \Rightarrow 1]\right| \leq 2k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},2}(\mathcal{B}) + \frac{1}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. The reduction is the reverse of Lemma 17. We use a Q_e-fold $\mathcal{U}_{3k,k}$-MDDH assumption on $\mathbf{B}$ to switch in EVAL queries with $p = \hat{\imath}$ the distribution of $\mathbf{t}$ from uniform random in $\mathbb{Z}_q^{3k}$ to $\mathsf{Span}(\mathbf{B})$. □

Lemma 28 ($\mathsf{G}_{2,\hat{\imath},5} \rightsquigarrow \mathsf{G}_{2,\hat{\imath}+1,0}$)**.** *For $\hat{\imath} < L$*

$$\Pr[\mathsf{G}_{2,\hat{\imath},5} \Rightarrow 1] = \Pr[\mathsf{G}_{2,\hat{\imath}+1,0} \Rightarrow 1].$$

Proof. These two games are equivalent. □

Lemma 29 ($\mathsf{G}_{2,L,5} \rightsquigarrow \mathsf{G}_3$)**.**

$$\left|\Pr[\mathsf{G}_{2,L,5} \Rightarrow 1] - \Pr\left[\mathsf{G}^{\mathcal{A}}_3 \Rightarrow 1\right]\right| \leq \mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}) + \frac{2}{q-1}$$

Proof. In game $\mathsf{G}_{2,L,0}$ the value h_1 is computed honestly while in G_3 it is chosen uniformly random.

To bound the difference between these two games, we need a Q_c-fold $\mathcal{U}_k$-MDDH challenge $\left([\mathbf{D}]_1, [\mathbf{f}_1]_1, \ldots, [\mathbf{f}_{Q_c}]_1\right)$ to execute the reduction given in Figure 15.

The INIT and EVAL oracles are identical in both games and simulated correctly by the reduction, because they do not return anything depending on $\mathbf{x}'$. Assume that $\overline{\mathbf{D}}$ is invertible. This happens with probability at least $(1 - 1/(q-1))$. Write $\mathbf{f}_c =: \begin{pmatrix} \overline{\mathbf{D}}\mathbf{w}_c \\ \underline{\mathbf{D}}\mathbf{w}_c + r_c \end{pmatrix}$ where $\mathbf{w}_c$ is uniform random in $\mathbb{Z}_q^k$ and r_c is 0 or uniform random

$\underline{\text{INIT}_{\mathsf{MAC}}}$:
parse $\mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
$\mathbf{B} \xleftarrow{\$} \mathcal{U}_{3k,k}$
for $i \in \{1, \dots, L\},\ j \in \{1, \dots, i\alpha\},\ b \in \{0,1\}$ **do** $\mathbf{X}_{i,j,b} \xleftarrow{\$} \mathbb{Z}_q^{k \times 3k}$
$\mathbf{j}' \xleftarrow{\$} \mathbb{Z}_q^k$
// Implicit: $\mathbf{x}' := \mathbf{j}' + \left(\underline{\mathbf{D}}\overline{\mathbf{D}}^{-1}\right)^\top$
$\Phi : \mathcal{S}^{\leq L} \dashrightarrow \mathbb{G}_2^{4k} \times \mathbb{G}_2^{\leq k\alpha\left(L^2+L\right)}$
$\mathsf{dk} := \left([\mathbf{X}_{i,j,b}\mathbf{B}]_2\right)_{1 \leq i \leq L, 1 \leq j \leq i\alpha, b \in \{0,1\}}$
return $\left(\mathcal{PG}, [\mathbf{B}]_2, \mathsf{dk}\right)$

$\underline{\text{FINALIZE}_{\mathsf{MAC}}(\beta \in \{0,1\})}$:
return $\left(\bigcup_{\mathsf{m}^\star \in \mathcal{C}_\mathcal{M}} \mathsf{Prefix}(\mathsf{m}^\star) \cap \mathcal{Q}_\mathcal{M} = \emptyset\right) \wedge \beta$

$\underline{\text{EVAL}(\mathsf{m} \in \mathcal{S}^p)}$:
if $\mathsf{m} \in \mathcal{Q}_\mathcal{M}$ **then**
  return $\mathsf{RerandTag}(\mathsf{m}, \Phi(\mathsf{m}))$
$\mathcal{Q}_\mathcal{M} := \mathcal{Q}_\mathcal{M} \cup \{\mathsf{m}\}$
$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{t} := \mathbf{B}\mathbf{s}$
$\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^k$
for $i \in \{p+1, \dots, L\},\ j \in \{1, \dots, i\alpha\},\ b \in \{0,1\}$ **do** $\mathbf{d}_{i,j,b} := \mathbf{X}_{i,j,b}\mathbf{t}$
$\mathsf{tdk} := \left([\mathbf{d}_{i,j,b}]_2\right)_{p+1 \leq i \leq L, 1 \leq j \leq i\alpha, b \in \{0,1\}}$
return $\Phi(\mathsf{m}) := \left([\mathbf{t}]_2, [\mathbf{u}]_2, \mathsf{tdk}\right)$

$\underline{\text{CHAL}(\mathsf{m}^\star \in \mathcal{S}^p)}$:
$\mathcal{C}_\mathcal{M} := \mathcal{C}_\mathcal{M} \cup \{\mathsf{m}^\star\}$
Let this be the c-th CHAL query.
$\mathbf{h} := \overline{\mathbf{f}_c}$
$\mathbf{h}_0 := \sum_{i=1}^{p} \sum_{j=1}^{i\alpha} \mathbf{X}_{i,j,[\![\mathsf{m}^\star]\!]_j}^\top \mathbf{h}$
$h_1 := (\mathbf{j}')^\top \mathbf{h} + \underline{\mathbf{f}_c}$
return $\left([\mathbf{h}]_1, [\mathbf{h}_0]_1, [h_1]_T\right)$

Fig. 15. Reduction for the transition from $\mathsf{G}_{2,L,5}$ to G_3 to the Q_c-fold $\mathcal{U}_k$-MDDH challenge $\left([\mathbf{D}]_1, [\mathbf{f}_1]_1, \dots, [\mathbf{f}_{Q_c}]_1\right)$.

in $\mathbb{Z}_q$. In CHAL queries the reduction picks $\mathbf{h} := \overline{\mathbf{f}_c}$. Since $\overline{\mathbf{f}_c}$ is a uniform random vector, $\mathbf{h}$ is distributed correctly. Furthermore, h_1 is computed as:

$$h_1 := (\mathbf{j}')^\top \mathbf{h} + \underline{\mathbf{f}_c} = (\mathbf{j}')^\top \mathbf{h} + = \underline{\mathbf{D}}\overline{\mathbf{D}}^{-1}\overline{\mathbf{f}_c} + r_c = (\mathbf{x}')^\top \mathbf{h} + r_c\,.$$

If $r_c = 0$, we are simulating game $\mathsf{G}_{2,L,5}$. If r_c is uniform random we are simulating game G_3. □

SUMMARY. To prove Theorem 2, we combine Lemmata 15–29 to change h_1 from real to random and then apply all Lemmata (except Lemma 29) in reverse order to get to the $\mathsf{mHPR\text{-}CMA}_{\mathsf{rand}}$ game. □

B Tight Multi-challenge Security for the second LP MAC

This section deals with achieving tight security in the multi-challenge setting for the second HIBE from [32]. Again, the MAC, given in Figure 16, only differs in the parameter η, that is k here. Furthermore this MAC has identity space base set $\mathcal{S} = \{0,1\}^\alpha$ (for arbitrary $\alpha \in \mathbb{N}_+$) and uses $n = 3k$, $n' = k$, $\ell(p) = p$ and $\ell'(l,i) = 0$ for $i < p$ and $\ell'(l,i) = 2i\alpha$ for $i = p$. To match the formal definition, $\mathbf{X}_{i,j,b}$ should be renamed to $\mathbf{X}_{i,i,2j-b}$ and $f_{i,i,2j-b}(\mathsf{m}) := \left([\![\mathsf{m}_{|i}]\!]_j \stackrel{?}{=} b\right)$. Similar to construction 1, certain transitions require now an MDDH challenge in $\mathbb{G}_1$ that

$\underline{\mathsf{Gen}_{\mathsf{MAC}}(\mathbb{G}_2, q, P_2)}$:
$\mathbf{B} \xleftarrow{\$} \mathcal{U}_{3k,k}$
for $i \in \{1,\dots,L\},\ j \in \{1,\dots,i\alpha\},\ b \in \{0,1\}$ **do** $\mathbf{X}_{i,j,b} \xleftarrow{\$} \mathbb{Z}_q^{k\times 3k}$
$\mathbf{x}' \xleftarrow{\$} \mathbb{Z}_q^k$
return $\mathsf{sk}_{\mathsf{MAC}} := \big(\mathbf{B}, (\mathbf{X}_{i,j,b})_{1\le i\le L, 1\le j\le i\alpha, b\in\{0,1\}}, \mathbf{x}'\big)$

$\underline{\mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m} \in \mathcal{S}^p)}$:
parse $\mathsf{sk}_{\mathsf{MAC}} =: \big(\mathbf{B}, (\mathbf{X}_{i,j,b})_{1\le i\le L, 1\le j\le i\alpha, b\in\{0,1\}}, \mathbf{x}'\big)$
for $i \in \{1,\dots,p\}$ **do** $\mathbf{s}_i \xleftarrow{\$} \mathbb{Z}_q^k;\ \mathbf{t}_i := \mathbf{B}\mathbf{s}_i$
$\mathbf{u} := \sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{X}_{i,j,[\![\mathsf{m}]\!]_j}\mathbf{t}_i + \mathbf{x}'$
return $\Big(\big([\mathbf{t}_i]_2\big)_{1\le i\le p}, [\mathbf{u}]_2\Big)$

$\underline{\mathsf{Ver}_{\mathsf{MAC}}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m} \in \mathcal{S}^p, \tau)}$:
parse $\mathsf{sk}_{\mathsf{MAC}} =: \big(\mathbf{B}, (\mathbf{X}_{i,j,b})_{1\le i\le L, 1\le j\le i\alpha, b\in\{0,1\}}, \mathbf{x}'\big)$
parse $\tau =: \Big(\big([\mathbf{t}_i]_2\big)_{1\le i\le p}, [\mathbf{u}]_2\Big)$
return $\mathbf{u} \stackrel{?}{=} \sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{X}_{i,j,[\![\mathsf{m}]\!]_j}\mathbf{t}_i + \mathbf{x}'$

Fig. 16. The new multi-challenge tightly secure affine MAC with levels MAC_2.

are information theoretic in the single challenge setting. Moreover, the security loss increases by a factor of L compared to the single-challenge version. Compared to construction 1, construction 2 needs no user delegation keys, but this comes at the cost of larger ciphertexts.

Theorem 3 (Security of MAC_2). MAC_2 *is tightly* mHPR-CMA *secure under the* $\mathcal{U}_k$-MDDH *assumption for* $\mathbb{G}_1$ *and* $\mathbb{G}_2$*. More precisely, for all adversaries* $\mathcal{A}$ *there exist adversaries* $\mathcal{B}_1$ *and* $\mathcal{B}_2$ *with*

$$\begin{aligned}\mathsf{Adv}^{\mathsf{mhpr\text{-}cma}}_{\mathsf{MAC}_2,\mathsf{PGGen}}(\mathcal{A}) &\le (4k + 16k\alpha L)\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},2}(\mathcal{B}_1)\\ &+ \big(1 + k\alpha\big(L^2+L\big)\big)\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}_2) + \frac{8 + \frac{1}{2}\alpha(Q_c+2)\big(L^2+L\big)}{q-1} + \frac{2Q_e}{q^{2k}}\end{aligned}$$

and $T(\mathcal{B}_1) \approx T(\mathcal{B}_2) \approx T(\mathcal{A}) + (Q_e + Q_c)\cdot\mathsf{poly}(\lambda)$*, where* Q_e *resp.* Q_c *denotes the number of* Eval *resp.* Chal *queries of* $\mathcal{A}$ *and* poly *is a polynomial independent of* $\mathcal{A}$*.*

Proof. The proof uses a hybrid argument with the hybrids G_0 (the $\mathsf{mHPR\text{-}CMA}_{\mathsf{real}}$ game), G_1, G_2, $\mathsf{G}_{3,\hat{\jmath}}$, for $\hat{\jmath} \in \{0,\dots,L\alpha\}$, $\mathsf{G}_{3,\hat{\jmath},1}$ and $\mathsf{G}_{3,\hat{\jmath},3}$ for $\hat{\jmath} \in \{0,\dots,L\alpha-1\}$, $\mathsf{G}_{3,\hat{\jmath},1,\hat{\imath}}$ and $\mathsf{G}_{3,\hat{\jmath},2,\hat{\imath}}$ for $\hat{\jmath} \in \{0,\dots,L\alpha-1\}$ and $\hat{\imath} \in \{\lfloor \hat{\jmath}/\alpha \rfloor,\dots,L\}$ G_4 and finally G_5. The hybrids are given in Figure 17 and 18. A summary can be found in

Table 5. They make use of random functions $\mathsf{RF}_{i,\hat{\jmath}} : \{0,1\}^{\hat{\jmath}} \to \mathbb{Z}_q^{k\times 2k}$, $\mathsf{ZF}_{i,\hat{\jmath}}$, $\mathsf{OF}_{i,\hat{\jmath}} : \{0,1\}^{\hat{\jmath}} \to \mathbb{Z}_q^{k\times k}$, defined on-the-fly.

Hybrid	$\mathbf{t}_i$ uniform in	$r_{\mathbf{u}}(\mathsf{m},i)$	$r_{\mathbf{h}_0}(\mathsf{m},i)$	Transition
G_0	$\mathsf{Span}(\mathbf{B})$	0		Original game
G_1	$\mathsf{Span}(\mathbf{B})$	0		Identical
G_2	$\mathbb{Z}_q^{3k}$	0		$\mathcal{U}_k$-MDDH in $\mathbb{G}_2$
$\mathsf{G}_{3,\hat{\jmath}}$	$\mathbb{Z}_q^{3k}$	$\mathsf{RF}_{i,\hat{\jmath}}(\llbracket\mathsf{m}\rrbracket_{\mid\hat{\jmath}})(\mathbf{B}^\perp)^\top$		Identical
$\mathsf{G}_{3,\hat{\jmath},1}$		$\mathsf{RF}_{i,\hat{\jmath}}(\llbracket\mathsf{m}\rrbracket_{\mid\hat{\jmath}})(\mathbf{B}^\perp)^\top$		$\mathcal{U}_k$-MDDH in $\mathbb{G}_2$
$\mathsf{G}_{3,\hat{\jmath},1,\hat{\imath}}$	**if** $\llbracket\mathsf{m}\rrbracket_{\hat{\jmath}+1} = 0$ **then** $\mid \mathsf{Span}(\mathbf{B}\mid\mathbf{B}_0)$ **else** $\lfloor \mathsf{Span}(\mathbf{B}\mid\mathbf{B}_1)$	$\mathsf{ZF}_{i,g(\hat{\jmath}\boxed{+1},i)}\left(\llbracket\mathsf{m}\rrbracket_{\mid g(\hat{\jmath}\boxed{+1},i)}\right)(\mathbf{B}_0^*)^\top + \mathsf{OF}_{i,g(\hat{\jmath},i)}\left(\llbracket\mathsf{m}\rrbracket_{\mid g(\hat{\jmath},i)}\right)(\mathbf{B}_1^*)^\top$ $\boxed{\text{If } i<\hat{\imath}}$		$\mathcal{U}_k$-MDDH in $\mathbb{G}_1$
$\mathsf{G}_{3,\hat{\jmath},2,\hat{\imath}}$		$\mathsf{ZF}_{i,g(\hat{\jmath}+1,i)}\left(\llbracket\mathsf{m}\rrbracket_{\mid g(\hat{\jmath}+1,i)}\right)(\mathbf{B}_0^*)^\top + \mathsf{OF}_{i,g(\hat{\jmath}\boxed{+1},i)}\left(\llbracket\mathsf{m}\rrbracket_{\mid g(\hat{\jmath}\boxed{+1},i)}\right)(\mathbf{B}_1^*)^\top$ $\boxed{\text{If } i<\hat{\imath}}$		$\mathcal{U}_k$-MDDH in $\mathbb{G}_1$
$\mathsf{G}_{3,\hat{\jmath},3}$		$\mathsf{RF}_{i,\hat{\jmath}+1}(\llbracket\mathsf{m}\rrbracket_{\mid\hat{\jmath}+1})(\mathbf{B}^\perp)^\top$		Identical
$\mathsf{G}_{3,\hat{\jmath}+1}$	$\mathbb{Z}_q^{3k}$	$\mathsf{RF}_{i,\hat{\jmath}+1}(\llbracket\mathsf{m}\rrbracket_{\mid\hat{\jmath}+1})(\mathbf{B}^\perp)^\top$		$\mathcal{U}_k$-MDDH in $\mathbb{G}_2$
G_4	$\mathbb{Z}_q^{3k}$	unif. random	$\mathsf{RF}_{i,i\alpha}(\mathsf{m}_{\mid i})(\mathbf{B}^\perp)^\top$	Statistically close
G_5	$\mathbb{Z}_q^{3k}$	unif. random	$\mathsf{RF}_{i,i\alpha}(\mathsf{m}_{\mid i})(\mathbf{B}^\perp)^\top$	$\mathcal{U}_k$-MDDH in $\mathbb{G}_1$

Table 5. Summary of the hybrids of Figure 17 and 18. Non-duplicated Eval queries draw $\mathbf{t}_i$ from the set described by the second column and add the randomness $\sum_{i=1}^{p} r_{\mathbf{u}}(\mathsf{m},i)\mathbf{t}_i$ to $\mathbf{u}$ or choose $\mathbf{u}$ uniform random. The Chal query adds the term $r_{\mathbf{h}_0}(\mathsf{m}^\star,i)h$ to each $\mathbf{h}_{0,i}$. Throughout this table $g(\hat{\jmath},i) := \max\{\hat{\jmath}, i\alpha\}$. The background color indicates repeated transitions.

Lemma 30 ($\mathsf{G}_0 \rightsquigarrow \mathsf{G}_1$)**.**

$$\Pr\left[\mathsf{G}_0^{\mathcal{A}} \Rightarrow 1\right] = \Pr\left[\mathsf{G}_1^{\mathcal{A}} \Rightarrow 1\right]$$

Proof. In game G_1 each time the adversary queries a tag for a message m, where he queried a tag for m before, the adversary will get a rerandomized version of the first tag he queried. The RerandTag algorithm chooses $\mathbf{t}_i' := \mathbf{t}_i + \mathbf{B}\mathbf{s}_i'$, which is uniformly random in $\mathsf{Span}(\mathbf{B})$ independent of $\mathbf{t}$, because $\mathbf{s}_i'$ is uniform random in $\mathbb{Z}_q^k$. The RerandTag algorithm then computes $\mathbf{u}'$ such that all $\mathbf{t}_i'$ and $\mathbf{u}'$ form

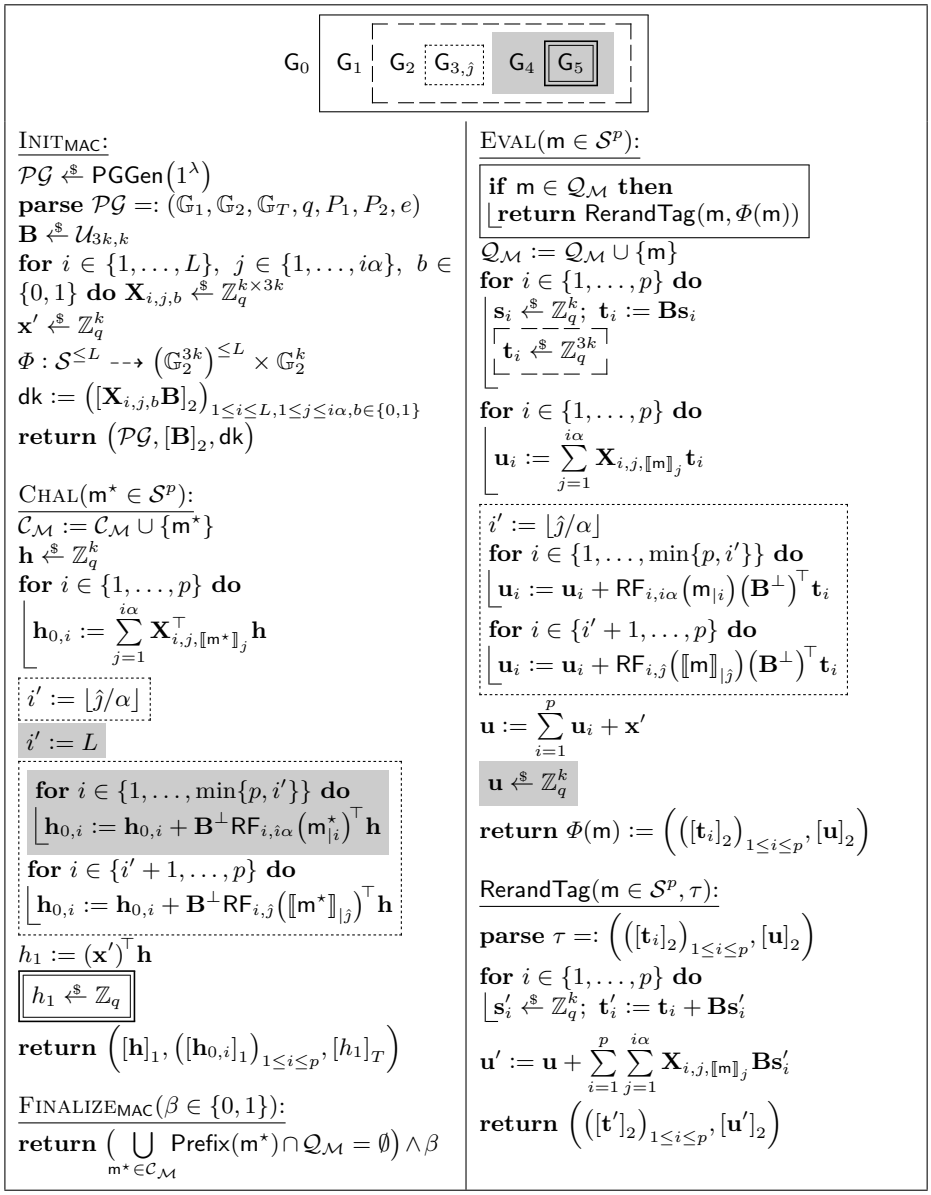


Fig. 17. Hybrids for the security proof of MAC_2. The algorithm $\mathsf{RerandTag}$ is only helper function and not an oracle for the adversary. The partial map Φ is initially totally undefined.

another valid tag for m, that is distributed like a fresh tag, independent of the input tag. Thus the games are equivalent.

Note that the rerandomization uses only the "public key" returned by the INIT oracle, so it could actually be carried out by the adversary herself. In the following, we will ignore these duplicated EVAL queries. □

Lemma 31 ($\mathsf{G}_1 \rightsquigarrow \mathsf{G}_2$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}_1^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_2^{\mathcal{A}} \Rightarrow 1\right]\right| \leq 2k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},2}(\mathcal{B}) + \frac{1}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. The only difference between these two games is, that the non-duplicated EVAL queries pick the vectors $\mathbf{t}_i$ uniformly random from $\mathbb{Z}_q^{3k}$ instead of only from $\mathsf{Span}(\mathbf{B})$. This leads to a straightforward reduction to a Q_eL-fold $\mathcal{U}_{3k,k}$-MDDH assumption on $\mathbf{B}$. By Lemma 3 the Q_eL-fold $\mathcal{U}_{3k,k}$-MDDH assumption is at most $2k$ times harder then the $\mathcal{U}_{3k,k}$-MDDH assumption and this assumption is equivalent to the $\mathcal{U}_k$-MDDH assumption by Lemma 1. □

Lemma 32 ($\mathsf{G}_2 \rightsquigarrow \mathsf{G}_{3,0}$)**.**

$$\Pr\left[\mathsf{G}_2^{\mathcal{A}} \Rightarrow 1\right] = \Pr\left[\mathsf{G}_{3,0}^{\mathcal{A}} \Rightarrow 1\right]$$

Proof. These two games are equivalent. When replacing in G_2 all the secret values $\mathbf{X}_{i,1,b}$ with $\mathbf{X}_{i,1,b} + \mathsf{RF}_{i,0}(\varepsilon)\left(\mathbf{B}^\perp\right)^\top$ (for $i \in \{1,\dots,L\}$ and $b \in \{0,1\}$), we get game $\mathsf{G}_{3,0}$. The distribution of $\mathbf{X}_{i,1,b}$ and $\mathbf{X}_{i,1,b} + \mathsf{RF}_{i,0}(\varepsilon)\left(\mathbf{B}^\perp\right)^\top$ is identical. Note that the term $\mathsf{RF}_{i,0}(\varepsilon)\left(\mathbf{B}^\perp\right)^\top$ cancels out in the master public key. □

Lemma 33 ($\mathsf{G}_{3,\hat{\jmath}} \rightsquigarrow \mathsf{G}_{3,\hat{\jmath}+1}$)**.** *For all $\hat{\jmath} \in \{0,\dots,L\alpha-1\}$ and all adversaries $\mathcal{A}$ there exist adversaries $\mathcal{B}_1$, $\mathcal{B}_2$ with*

$$\begin{aligned}\left|\Pr\left[\mathsf{G}_{3,\hat{\jmath}}^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_{3,\hat{\jmath}+1}^{\mathcal{A}} \Rightarrow 1\right]\right| &\leq 8k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},2}(\mathcal{B}_2) \\ &\quad + k(L-i')\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}_1) + \frac{4 + (Q_c+2)(L-i')}{q-1},\end{aligned}$$

where $i' := \lfloor \hat{\jmath}/\alpha \rfloor$ and $T(\mathcal{B}_1) \approx T(\mathcal{B}_2) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. To prove this transition, we use the hybrids $\mathsf{G}_{3,\hat{\jmath},1}$, $\mathsf{G}_{3,\hat{\jmath},1,\hat{\imath}}$ and $\mathsf{G}_{3,\hat{\jmath},2,\hat{\imath}}$ for $\hat{\imath} \in \{i',\dots,L\}$ and $\mathsf{G}_{3,\hat{\jmath},3}$. The hybrids are given in Figure 18.

Lemma 33 follows directly from Lemmata 34–40. □

Lemma 34 ($\mathsf{G}_{3,\hat{\jmath}} \rightsquigarrow \mathsf{G}_{3,\hat{\jmath},1}$)**.**

$$\left|\Pr\left[\mathsf{G}_{3,\hat{\jmath}}^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_{3,\hat{\jmath},1}^{\mathcal{A}} \Rightarrow 1\right]\right| \leq 4k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},2}(\mathcal{B}) + \frac{2}{q-1}$$

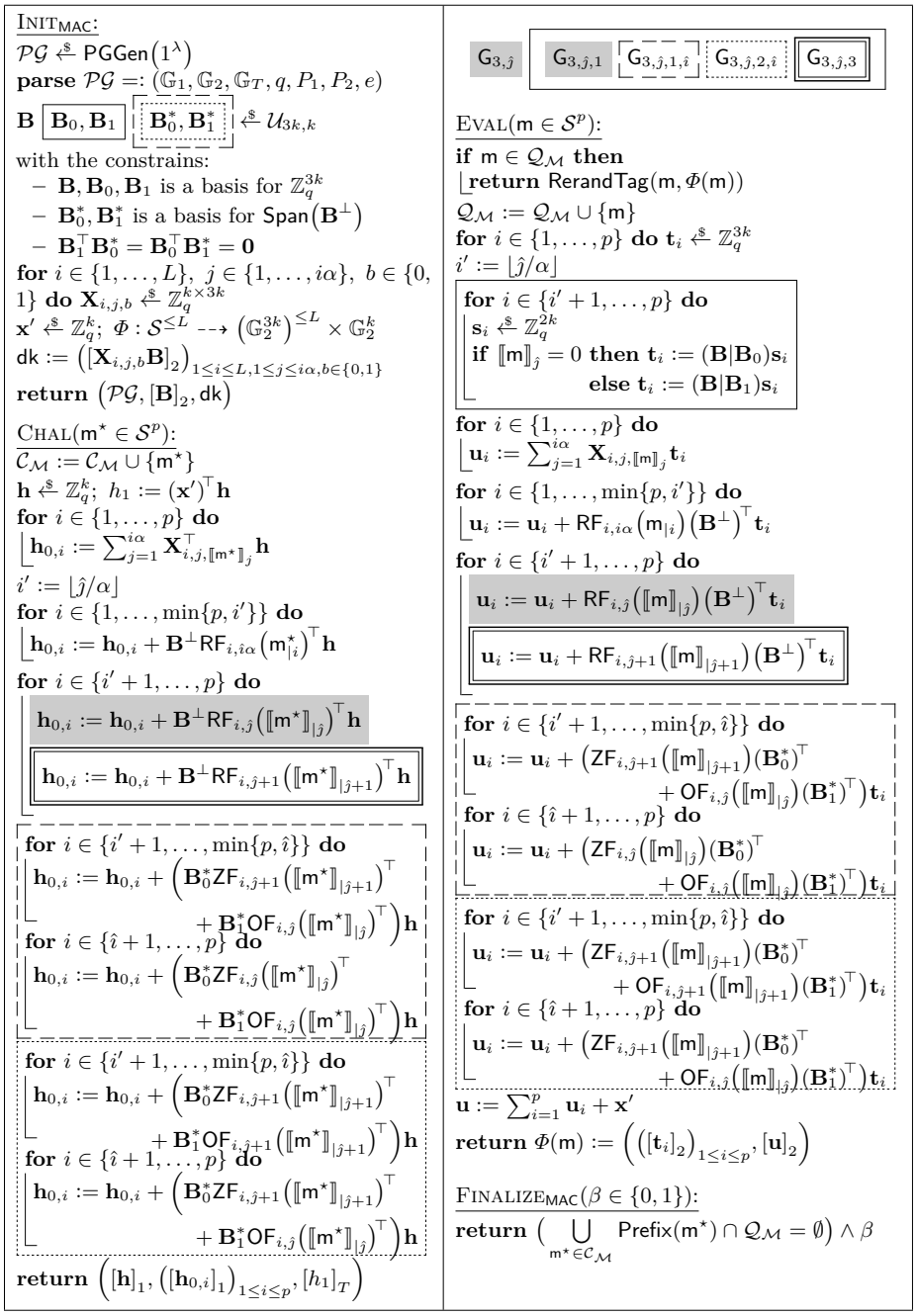


Fig. 18. Hybrids for the transition from $\mathsf{G}_{3,\hat{\jmath}}$ to $\mathsf{G}_{3,\hat{\jmath}+1}$. The algorithm $\mathsf{RerandTag}$ is defined in Figure 17.

Proof. These two games are equivalent except that in the EVAL queries the vectors $\mathbf{t}_i$ (for $i \geq i' + 1$) are generated uniformly random from $\mathbb{Z}_q^{3k}$ in game $\mathsf{G}_{3,\hat{\jmath}}$ and from either $\mathsf{Span}(\mathbf{B}|\mathbf{B}_0)$ or $\mathsf{Span}(\mathbf{B}|\mathbf{B}_1)$ depending on the bit $[\![\mathsf{m}]\!]_{\hat{\jmath}+1}$ in game $\mathsf{G}_{3,\hat{\jmath},1}$. We can switch from $\mathsf{G}_{3,\hat{\jmath}}$ to $\mathsf{G}_{3,\hat{\jmath},1}$ with two $Q_e L$-fold $\mathcal{U}_{3k,k}$-MDDH challenges.

The proof is analogous to Lemma 20. □

Lemma 35 ($\mathsf{G}_{3,\hat{\jmath},1} \rightsquigarrow \mathsf{G}_{3,\hat{\jmath},1,i'}$)**.** *Let* $i' := \lfloor \hat{\jmath}/\alpha \rfloor$.

$$\Pr\left[\mathsf{G}^{\mathcal{A}}_{3,\hat{\jmath},1} \Rightarrow 1\right] = \Pr\left[\mathsf{G}^{\mathcal{A}}_{3,\hat{\jmath},1,i'} \Rightarrow 1\right]$$

Proof. These two games are equivalent. In game $\mathsf{G}_{3,\hat{\jmath},1,i'}$ we have only replaced $\mathsf{RF}_{i,\hat{\jmath}}\left([\![\mathsf{m}]\!]_{|\hat{\jmath}}\right)\left(\mathbf{B}^{\perp}\right)^{\top}$ with $\mathsf{ZF}_{i,\hat{\jmath}}\left([\![\mathsf{m}]\!]_{|\hat{\jmath}}\right)\left(\mathbf{B}_0^*\right)^{\top} + \mathsf{OF}_{i,\hat{\jmath}}\left([\![\mathsf{m}]\!]_{|\hat{\jmath}}\right)\left(\mathbf{B}_1^*\right)^{\top}$ compared to game $\mathsf{G}_{3,\hat{\jmath},1}$. But this does not change the distribution, since $\mathbf{B}_0^*, \mathbf{B}_1^*$ is a basis of $\mathsf{Span}\left(\mathbf{B}^{\perp}\right)$. □

Lemma 36 ($\mathsf{G}_{3,\hat{\jmath},1,\hat{\imath}} \rightsquigarrow \mathsf{G}_{3,\hat{\jmath},1,\hat{\imath}+1}$)**.** *For all adversaries* $\mathcal{A}$ *there exists an adversary* $\mathcal{B}$ *with*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{3,\hat{\jmath},1,\hat{\imath}} \Rightarrow 1\right] - \Pr[\mathsf{G}_{3,\hat{\jmath},1,\hat{\imath}+1} \Rightarrow 1]\right| \leq k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}) + \frac{Q_c + 2}{q - 1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. The proof is analogous to Lemma 21. □

Lemma 37 ($\mathsf{G}_{3,\hat{\jmath},1,L} \rightsquigarrow \mathsf{G}_{3,\hat{\jmath},2,i'}$)**.** *Let* $i' := \lfloor \hat{\jmath}/\alpha \rfloor$.

$$\Pr\left[\mathsf{G}^{\mathcal{A}}_{3,\hat{\jmath},1,L} \Rightarrow 1\right] = \Pr\left[\mathsf{G}^{\mathcal{A}}_{3,\hat{\jmath},2,i'} \Rightarrow 1\right]$$

Proof. The games are equivalent. □

Lemma 38 ($\mathsf{G}_{3,\hat{\jmath},2,\hat{\imath}} \rightsquigarrow \mathsf{G}_{3,\hat{\jmath},2,\hat{\imath}+1}$)**.** *For all adversaries* $\mathcal{A}$ *there exists an adversary* $\mathcal{B}$ *with*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{3,\hat{\jmath},1,\hat{\imath}} \Rightarrow 1\right] - \Pr[\mathsf{G}_{3,\hat{\jmath},1,\hat{\imath}+1} \Rightarrow 1]\right| \leq k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}) + \frac{Q_c + 2}{q - 1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. The proof is analogous to Lemma 22. □

Remark 1. Analogous to Lemma 23, we can reduce the number of necessary MDDH challenges in $\mathbb{G}_1$ by one half by simultaneously adding one more input bit to $\mathsf{ZF}_{i,\cdot}$ and $\mathsf{OF}_{i,\cdot}$.

Lemma 39 ($\mathsf{G}_{3,\hat{\jmath},2,L} \rightsquigarrow \mathsf{G}_{3,\hat{\jmath},3}$)**.** *Let* $i' := \lfloor \hat{\jmath}/\alpha \rfloor$.

$$\Pr[\mathsf{G}_{3,\hat{\jmath},2,L} \Rightarrow 1] = \Pr[\mathsf{G}_{3,\hat{\jmath},3} \Rightarrow 1]$$

Proof. These two games are equivalent. In game $\mathsf{G}_{3,\hat{\jmath},3}$ we have only replaced $\mathsf{ZF}_{i,\hat{\jmath}+1}\left(\llbracket \mathsf{m} \rrbracket_{|\hat{\jmath}+1}\right)(\mathbf{B}_0^*)^\top + \mathsf{OF}_{i,\hat{\jmath}+1}\left(\llbracket \mathsf{m} \rrbracket_{|\hat{\jmath}+1}\right)(\mathbf{B}_1^*)^\top$ with $\mathsf{RF}_{i,\hat{\jmath}+1}\left(\llbracket \mathsf{m} \rrbracket_{|\hat{\jmath}+1}\right)\left(\mathbf{B}^\perp\right)^\top$ compared to game $\mathsf{G}_{3,\hat{\jmath},2,L}$. But this does not change the distribution, since $\mathbf{B}_0^*, \mathbf{B}_1^*$ is a basis of $\mathsf{Span}\left(\mathbf{B}^\perp\right)$ □

Lemma 40 ($\mathsf{G}_{3,\hat{\jmath},3} \rightsquigarrow \mathsf{G}_{3,\hat{\jmath}+1}$)**.** *For $\hat{\jmath} < L\alpha$ and all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}_{3,\hat{\jmath},3}^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_{3,\hat{\jmath}+1}^{\mathcal{A}} \Rightarrow 1\right]\right| \leq 4k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},2}(\mathcal{B}) + \frac{2}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. The transition is the reverse of Lemma 34. □

Lemma 41 ($\mathsf{G}_{3,L\alpha} \rightsquigarrow \mathsf{G}_4$)**.**

$$\left|\Pr\left[\mathsf{G}_{3,L\alpha}^{\mathcal{A}} \Rightarrow 1\right] - \Pr[\mathsf{G}_4 \Rightarrow 1]\right| \leq \frac{Q_e}{q^{2k}}$$

Proof. Assume $\forall \mathsf{m}^\star \in \mathcal{C}_{\mathcal{M}} : \mathsf{Prefix}(\mathsf{m}^\star) \cap \mathcal{Q}_{\mathcal{M}} \neq \emptyset$, otherwise the adversary has lost the game anyway. In each user secret key query the value $\mathsf{RF}_{p,p\alpha}(\mathsf{m})\left(\mathbf{B}^\perp\right)^\top \mathbf{t}_p$ is added to $\mathbf{u}$. This is the only place where $\mathsf{RF}_{p,p\alpha}(\mathsf{m})\left(\mathbf{B}^\perp\right)^\top$ is used, since only the first Eval query for each message evaluates the random function and Chal queries evaluate $\mathsf{RF}_{p,p\alpha}$ only on prefixes of $\mathsf{m}^\star \in \mathcal{C}_{\mathcal{M}}$. Thus each non-duplicated Eval query outputs a uniformly random vector for $\mathbf{u}$ when $\mathbf{t}_p \notin \mathsf{Span}(\mathbf{B})$, which happens with probability at least $(1 - 1/(q^{2k}))$. In this case the games are distributed identically. □

Lemma 42 ($\mathsf{G}_4 \rightsquigarrow \mathsf{G}_5$)**.**

$$\left|\Pr\left[\mathsf{G}_4^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_5^{\mathcal{A}} \Rightarrow 1\right]\right| \leq \mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}) + \frac{2}{q-1}$$

Proof. The proof is analogous to Lemma 29. □

Summary. To prove Theorem 3, we combine Lemmata 30–42 to change h_1 from real to random and then apply all Lemmas (except Lemma 42) in reverse order to get to the $\mathsf{mHPR\text{-}CMA}_{\mathsf{rand}}$ game. □

C Anonymous Delegatable Affine MACs

C.1 Definition

To achieve mPR-HID-CPA security (and thus anonymity) for HIBKEMs, the underlying MAC needs to satisfy the mAPR-CMA security notion from [5]. We recap this definition for delegatable affine MACs here for completeness.[4] Basically,

[4] There is no need to generalize this notion for affine MACs with levels since we will only proof anonymity for the first MAC, that is a delegatable affine MAC.

$\underline{\text{INIT}_{\mathsf{MAC}}}$:
$\mathcal{PG} \xleftarrow{\$} \mathsf{PGGen}\left(1^\lambda\right)$
parse $\mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
$\mathsf{sk}_{\mathsf{MAC}} \xleftarrow{\$} \mathsf{Gen}_{\mathsf{MAC}}(\mathbb{G}_2, q, P_2)$
$\mathsf{sk}_{\mathsf{MAC}} =: \left(\mathbf{B}, (\mathbf{X}_{l,i,j})_{\substack{1 \le l \le \ell(p), 1 \le i \le L, \\ 1 \le j \le \ell'(l,i)}}, \mathbf{x}'\right)$
return $\mathcal{PG}$

$\underline{\text{CHAL}(\mathsf{m}^\star \in \mathcal{S}^p)}$:
$\mathcal{C}_{\mathcal{M}} := \mathcal{C}_{\mathcal{M}} \cup \{\mathsf{m}^\star\}$
$\mathbf{h} \xleftarrow{\$} \mathbb{Z}_q^\eta$
$\mathbf{h}_0 := \left(\sum_{i=1}^{L} \sum_{j=1}^{\ell'(i)} f_{i,j}\left(\mathsf{m}^\star_{|i}\right) \mathbf{X}_{i,j}^\top\right) \mathbf{h}$
$h_1 = (\mathbf{x}')^\top \mathbf{h} \in \mathbb{Z}_q$
$\boxed{h_1 \xleftarrow{\$} \mathbb{Z}_q}$
return $\left([\mathbf{h}]_1, [\mathbf{h}_0]_1, [h_1]_T\right)$

$\underline{\text{EVAL}(\mathsf{m} \in \mathcal{S}^p)}$:
$\mathcal{Q}_{\mathcal{M}} := \mathcal{Q}_{\mathcal{M}} \cup \{\mathsf{m}\}$
$\left([\mathbf{t}]_2, [\mathbf{u}]_2\right) \xleftarrow{\$} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m})$
$\mathbf{S} \xleftarrow{\$} \mathsf{GL}_{n'}(\mathbb{Z}_q)$; $\mathbf{T} := \mathbf{BS}$
$\mathbf{U} := \sum_{i=1}^{p} \sum_{j=1}^{\ell'(i)} f_{i,j}\left(\mathsf{m}_{|i}\right) \mathbf{X}_{i,j} \mathbf{T}$
for $i \in \{p{+}1, \ldots, L\}$, $j \in \{1, \ldots, \ell'(l,i)\}$ **do**
  $\mathbf{d}_{i,j} := \mathbf{X}_{i,j}\mathbf{t}$; $\mathbf{D}_{i,j} := \mathbf{X}_{i,j}\mathbf{T}$
$\mathsf{tdk} := \left([\mathbf{d}_{l,i,j}]_2, [\mathbf{D}_{l,i,j}]_2\right)_{\substack{p+1 \le i, \le L \\ 1 \le j \le \ell'(i)}}$
return $\left([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{T}]_2, [\mathbf{U}]_2, \mathsf{tdk}\right)$

$\underline{\text{FINALIZE}_{\mathsf{MAC}}(\beta \in \{0,1\})}$:
return $\left(\bigcup_{\mathsf{m}^\star \in \mathcal{C}_{\mathcal{M}}} \mathsf{Prefix}(\mathsf{m}^\star) \cap \mathcal{Q}_{\mathcal{M}} = \emptyset\right) \wedge \beta$

Fig. 19. Games $\mathsf{mAPR\text{-}CMA}_{\mathsf{real}}$ and $\boxed{\mathsf{mAPR\text{-}CMA}_{\mathsf{rand}}}$ for defining mAPR-CMA security for delegatable affine MACs.

this notion requires that the vector $\mathbf{h}_0$ is also pseudorandom to the adversary. However, this can not be achieved when the adversary knows the matrices $\left[\mathbf{X}_{i,j}^\top \mathbf{B}\right]_2$, that are given to him in INIT in the mPR-CMA game. Thus, the mAPR-CMA games use a different tag rerandomization mechanism. They are defined in Figure 19. Compared to the original definition of [5], we require the matrix $\mathbf{S}$ in the EVAL oracle to be invertible, to ensure the rerandomized tags are exactly distributed like fresh tags and not only statistical close.

Definition 8 (mAPR-CMA Security). *An affine MAC (with levels)* MAC *is* mAPR-CMA-secure *in* $\mathbb{G}_2$ *if for all PPT adversaries* $\mathcal{A}$ *the function*

$$\mathsf{Adv}^{\mathsf{mapr\text{-}cma}}_{\mathsf{MAC}}(\mathcal{A}) := \left|\Pr\left[\mathsf{mAPR\text{-}CMA}^{\mathcal{A}}_{\mathsf{real}} \Rightarrow 1\right] - \Pr\left[\mathsf{mAPR\text{-}CMA}^{\mathcal{A}}_{\mathsf{rand}} \Rightarrow 1\right]\right|$$

is negligible.

C.2 Construction

The delegatable affine MAC MAC_1 is mAPR-CMA-secure. Thus it can be transformed to an anonymous HIBE scheme with the anonymity-preserving transformation from [5]. We recap the transformation in Appendix E for completeness. The resulting anonymous HIBE's user secret keys are larger (by a constant factor) compared to the HIBE obtained from the non-anonymous transformation. A comparison of the resulting HIBE with other anonymous HIBEs can be found in Table 6.

Scheme	$\lvert\mathsf{mpk}\rvert$	$\lvert\mathsf{usk}\rvert$	$\lvert\mathsf{C}\rvert$	Loss	MC	Ass.
BW06 [8]	$\mathbf{O}(L^2)\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(L^2)\lvert\mathbb{G}_2\rvert$	$(2p+5)\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(Q_\mathsf{e}L^2)$	✗	DBDH
Duc10 [12]	$\mathbf{O}(L)(\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert)$	$\mathbf{O}(L^2)\lvert\mathbb{G}_2\rvert$	$(p+2)\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(L)$	✗	$\mathcal{P}$-BDH
OT12 [39]	$160\lvert\mathbb{G}\rvert$	$\mathbf{O}(p^2L)\lvert\mathbb{G}\rvert$	$3+6p\lvert\mathbb{G}\rvert$	$\mathbf{O}(Q_\mathsf{e}L^2)$	✗	2-LIN
BKP14 [5]	$\mathbf{O}(Lk^2)\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(Lk^2)\lvert\mathbb{G}_2\rvert$	$(2k+2)\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(Q_\mathsf{e})$	✗	k-LIN
HIBKEM_3	$\mathbf{O}(nL^2k^2)\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(nL^2k^2)\lvert\mathbb{G}_2\rvert$	$5k\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(nL^2k)$	✓	k-LIN
$\mathsf{HIBKEM}_3^{\mathcal{H}}$	$\mathbf{O}(\gamma Lk^2)\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(\gamma Lk^2)\lvert\mathbb{G}_2\rvert$	$5k\lvert\mathbb{G}_1\rvert$	$\mathbf{O}(\gamma Lk)$	✓	k-LIN

Table 6. Comparison of anonymous HIBEs in prime-order pairing groups in the standard model based on static assumptions. The schemes BW06 and Duc10 are selectively secure, the other ones are adaptively secure. The highlighted rows are from this paper. HIBKEM_3 can be found in Figure 42. $\mathsf{HIBKEM}_3^{\mathcal{H}}$ is obtained by hashing the identities as described in the full version of [32].
The identity space is $(\{0,1\}^n)^{\leq L}$ and γ is the bit length of the range of a collision-resistant hash function. '$\lvert\mathsf{mpk}\rvert$,' '$\lvert\mathsf{usk}\rvert$,' and '$\lvert\mathsf{C}\rvert$' stand for the size of the master public key, a user secret key and a ciphertext, respectively. We count the number of group elements in $\mathbb{G}_1, \mathbb{G}_2$, and $\mathbb{G}_T$. For a scheme that works in symmetric pairing groups, we write $\mathbb{G}(:= \mathbb{G}_1 = \mathbb{G}_2)$. The schemes that work in asymmetric pairing groups can be instantiated with SXDH=1-LIN. In the '$\lvert\mathsf{usk}\rvert$' and '$\lvert\mathsf{C}\rvert$' columns p stands for the hierarchy depth of the identity vector. In bounded HIBEs, L denotes the maximum hierarchy depth. In the security loss, Q_e denotes the number of user secret key queries by the adversary. The last but one column indicates whether the adversary is allowed to query multiple challenge ciphertexts (✓) or just one (✗). The last column shows the underlying security assumption.

Theorem 4 (Anonymity of MAC_1). MAC_1 *is tightly* mAPR-CMA *secure in* $\mathbb{G}_2$ *under the* $\mathcal{U}_k$-MDDH *assumption for* $\mathbb{G}_1$ *and* $\mathbb{G}_2$*. More precisely, for all adversaries* $\mathcal{A}$ *there exist adversaries* $\mathcal{B}_1$ *and* $\mathcal{B}_2$ *with*

$$\begin{aligned}\mathsf{Adv}^{\mathsf{mapr\text{-}cma}}_{\mathsf{MAC}_1}(\mathcal{A}) \leq{}& \big(8k(\alpha+1)L + 8k\alpha L^2\big)\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},2}(\mathcal{B}_1)\\ &+ \left(1+3k+2kL+\frac{1}{2}k\alpha\big(L+L^2\big)\right)\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}_2)\\ &+ \frac{4+4L+2Q_e+(5+Q_c/2)\alpha\big(L+L^2\big)}{q-1} + \frac{2Q_e}{q^{k-1}(q-1)}\end{aligned}$$

and $T(\mathcal{B}_1) \approx T(\mathcal{B}_2) \approx T(\mathcal{A}) + (Q_e+Q_c)\cdot\mathsf{poly}(\lambda)$*, where* Q_e *resp.* Q_c *denotes the number of* Eval *resp.* Chal *queries of* $\mathcal{A}$ *and* poly *is a polynomial independent of* $\mathcal{A}$*.*

Proof. The proof uses a hybrid argument with the hybrids G_0 (the $\mathsf{mAPR\text{-}CMA}_{\mathsf{real}}$ game), G_1, G_2, $\mathsf{G}_{3,\hat{\imath},0}$, $\mathsf{G}_{3,\hat{\imath},1}$ and $\mathsf{G}_{3,\hat{\imath},3}$–$\mathsf{G}_{3,\hat{\imath},5}$ for $\hat{\imath} \in \{1,\ldots,L\}$, $\mathsf{G}_{3,\hat{\imath},2,\hat{\jmath},0}$ for $\hat{\imath} \in \{1,\ldots,L\}$ and $\hat{\jmath} \in \{0,\ldots,\hat{\imath}\alpha\}$, $\mathsf{G}_{3,\hat{\imath},2,\hat{\jmath},1}$–$\mathsf{G}_{3,\hat{\imath},2,\hat{\jmath},3}$ for $\hat{\imath} \in \{1,\ldots,L\}$ and $\hat{\jmath} \in \{0,\ldots,\hat{\imath}\alpha-1\}$, G_4 and finally G_5. The hybrids are given in Figure 20 and

21. A summary can be found in Table 7. They make use of random functions $\mathsf{RF}_{\hat{\imath},\hat{\jmath}} : \{0,1\}^{\hat{\jmath}} \to \mathbb{Z}_q^{k\times 2k}$, $\mathsf{ZF}_{\hat{\imath},\hat{\jmath}}, \mathsf{OF}_{\hat{\imath},\hat{\jmath}} : \{0,1\}^{\hat{\jmath}} \to \mathbb{Z}_q^{k\times k}$, defined on-the-fly.

Hybrid	$(\mathbf{t}\|\mathbf{T})$ uniform in	$r_{\mathbf{u}}(\mathsf{m})$	$r_{\mathbf{h}_0}(\mathsf{m})$	Transition
G_0	$(\mathsf{Span}(\mathbf{B})\|\mathsf{GL}_k(\mathbb{Z}_q))$	0		Original game
G_1	$(\mathsf{Span}(\mathbf{B})\|\mathsf{GL}_k(\mathbb{Z}_q))$	0		Identical
G_2	$\mathsf{Span}(\mathbf{B})^{k+1}$	0		Statistically close
$\mathsf{G}_{3,\hat{\imath},0}$	$\mathsf{Span}(\mathbf{B})^{k+1}$	0		Identical
$\mathsf{G}_{3,\hat{\imath},1}$	$\left(\mathbb{Z}_q^{3k}\right)^{k+1}$	0		$\mathcal{U}_k$-MDDH in $\mathbb{G}_2$
$\mathsf{G}_{3,\hat{\imath},2,\hat{\jmath},0}$	$\left(\mathbb{Z}_q^{3k}\right)^{k+1}$	$\mathsf{RF}_{\hat{\imath},\hat{\jmath}}\left(\llbracket\mathsf{m}\rrbracket_{\|\hat{\jmath}}\right)\left(\mathbf{B}^{\perp}\right)^{\top}$		Identical
$\mathsf{G}_{3,\hat{\imath},2,\hat{\jmath},1}$	**if** $\llbracket\mathsf{m}\rrbracket_{\hat{\jmath}+1} = 0$ **then** $\mathsf{Span}(\mathbf{B}\|\mathbf{B}_0)^{k+1}$ **else** $\mathsf{Span}(\mathbf{B}\|\mathbf{B}_1)^{k+1}$	$\mathsf{RF}_{\hat{\imath},\hat{\jmath}}\left(\llbracket\mathsf{m}\rrbracket_{\|\hat{\jmath}}\right)\left(\mathbf{B}^{\perp}\right)^{\top}$		$\mathcal{U}_k$-MDDH in $\mathbb{G}_2$
$\mathsf{G}_{3,\hat{\imath},2,\hat{\jmath},2}$		$\left(\mathsf{ZF}_{\hat{\imath},\hat{\jmath}+1}\left(\llbracket\mathsf{m}\rrbracket_{\|\hat{\jmath}+1}\right)(\mathbf{B}_0^*)^{\top} + \mathsf{OF}_{\hat{\imath},\hat{\jmath}}\left(\llbracket\mathsf{m}\rrbracket_{\|\hat{\jmath}}\right)(\mathbf{B}_1^*)^{\top}\right)$		$\mathcal{U}_k$-MDDH in $\mathbb{G}_1$
$\mathsf{G}_{3,\hat{\imath},2,\hat{\jmath},3}$		$\left(\mathsf{ZF}_{\hat{\imath},\hat{\jmath}+1}\left(\llbracket\mathsf{m}\rrbracket_{\|\hat{\jmath}+1}\right)(\mathbf{B}_0^*)^{\top} + \mathsf{OF}_{\hat{\imath},\hat{\jmath}+1}\left(\llbracket\mathsf{m}\rrbracket_{\|\hat{\jmath}+1}\right)(\mathbf{B}_1^*)^{\top}\right)$		$\mathcal{U}_k$-MDDH in $\mathbb{G}_1$
$\mathsf{G}_{3,\hat{\imath},2,\hat{\jmath}+1,0}$	$\left(\mathbb{Z}_q^{3k}\right)^{k+1}$	$\mathsf{RF}_{\hat{\imath},\hat{\jmath}+1}\left(\llbracket\mathsf{m}\rrbracket_{\|\hat{\jmath}+1}\right)\left(\mathbf{B}^{\perp}\right)^{\top}$		$\mathcal{U}_k$-MDDH in $\mathbb{G}_2$
$\mathsf{G}_{3,\hat{\imath},3}$	$\left(\mathbb{Z}_q^{3k}\right)^{k+1}$	uniform random	$\mathsf{RF}_{\hat{\imath}}\left(\mathsf{m}_{\|\hat{\imath}}\right)\left(\mathbf{B}^{\perp}\right)^{\top}$	Statistically close
$\mathsf{G}_{3,\hat{\imath},4}$	$\left(\mathbb{Z}_q^{3k}\right)^{k+1}$	uniform random	0	$\mathcal{U}_k$-MDDH in $\mathbb{G}_1$
$\mathsf{G}_{3,\hat{\imath},5}$	$\mathsf{Span}(\mathbf{B})^{k+1}$	uniform random	0	$\mathcal{U}_k$-MDDH in $\mathbb{G}_2$
G_4	$\mathsf{Span}(\mathbf{B})^{k+1}$	uniform random	uniform random	$\mathcal{U}_k$-MDDH in $\mathbb{G}_1$
G_5	$\mathsf{Span}(\mathbf{B})^{k+1}$	uniform random	uniform random	$\mathcal{U}_k$-MDDH in $\mathbb{G}_1$

Table 7. Summary of the hybrids of Figure 20 and 21. Non-duplicated Eval queries (with $p = \hat{\imath}$) draw $\mathbf{t}$ and $\mathbf{T}$ from the set described by the second column and add the randomness $r_{\mathbf{u}}(\mathsf{m})\mathbf{t}$ to $\mathbf{u}$ and add $r_{\mathbf{u}}(\mathsf{m})\mathbf{T}$ to $\mathbf{U}$ or choose $\mathbf{u}$ and $\mathbf{U}$ uniform random. The Chal queries add the term $r_{\mathbf{h}_0}(\mathsf{m}^\star)^\top\mathbf{h}$ to $\mathbf{h}_0$ (if $\mathsf{m}^\star$ has length $\geq \hat{\imath}$). The column "Transition" displays how we can switch to this hybrid from the previous one. The background colors indicate repeated transitions.

Lemma 43 ($\mathsf{G}_0 \rightsquigarrow \mathsf{G}_1$)**.**

$$\Pr\left[\mathsf{G}_0^{\mathcal{A}} \Rightarrow 1\right] = \Pr\left[\mathsf{G}_1^{\mathcal{A}} \Rightarrow 1\right]$$

Proof. In game G_1 each time the adversary queries a tag for a message m, where he queried a tag for m before, the adversary will get a rerandomized version of the first tag he queried. The $\mathsf{RerandTag}$ algorithm chooses $\mathbf{t}' := \mathbf{t} + \mathbf{T}\mathbf{s}'$, which is uniformly random in $\mathsf{Span}(\mathbf{B})$ and independent of $\mathbf{t}$ and $\mathbf{T}$, since $\mathbf{s}'$ is uniform

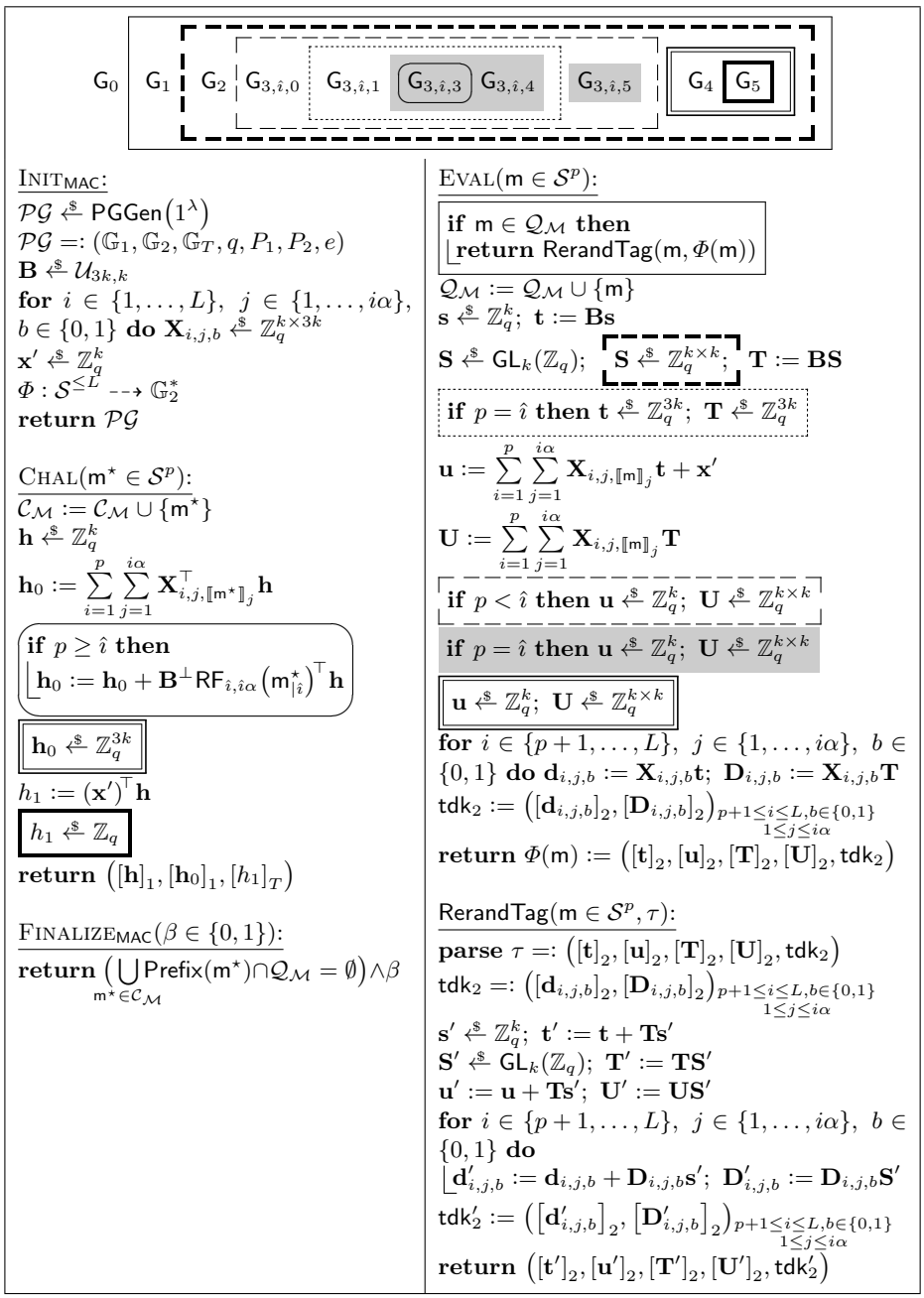


Fig. 20. Hybrids for the mAPR-CMA-security proof of MAC_1. The algorithm RerandTag is only helper function and not an oracle for the adversary. The partial map Φ is initially totally undefined.

random in $\mathbb{Z}_q^k$ and $\mathbf{T} = \mathbf{BS}$ for an invertible matrix $\mathbf{S}$. Furthermore the algorithm chooses $\mathbf{T}' := \mathbf{TS}'$ for an invertible matrix $\mathbf{S}'$, so $\mathbf{T}'$ is distributed correctly.

Note that the rerandomization uses only the input tag, so it could actually be carried out by the adversary herself. In the following we will ignore these duplicated Eval queries. □

Lemma 44 ($\mathsf{G}_1 \rightsquigarrow \mathsf{G}_2$)**.**

$$\left|\Pr\left[\mathsf{G}_1^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_2^{\mathcal{A}} \Rightarrow 1\right]\right| \leq \frac{Q_e}{q-1}$$

Proof. In game G_2 $\mathbf{S}$ is chosen uniformly random from $\mathbb{Z}_q^{k\times k}$ instead of $\mathsf{GL}_k(\mathbb{Z}_q)$. With probability at least $(1 - 1/(q-1))$ a matrix uniformly random in $\mathbb{Z}_q^{k\times k}$ is invertible and then the adversary can not notice any difference between these two games. □

Lemma 45 ($\mathsf{G}_2 \rightsquigarrow \mathsf{G}_{3,1,0}$)**.**

$$\Pr\left[\mathsf{G}_2^{\mathcal{A}} \Rightarrow 1\right] = \Pr\left[\mathsf{G}_{3,1,0}^{\mathcal{A}} \Rightarrow 1\right]$$

Proof. These two games are equivalent. □

Lemma 46 ($\mathsf{G}_{3,\hat{\imath},0} \rightsquigarrow \mathsf{G}_{3,\hat{\imath},1}$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}_{3,\hat{\imath},0}^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_{3,\hat{\imath},1}^{\mathcal{A}} \Rightarrow 1\right]\right| \leq 2k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},2}(\mathcal{B}) + \frac{1}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. These two games are equivalent except that in Eval-queries with $p = \hat{\imath}$ the $\mathbf{t}$ and the column vectors of $\mathbf{T}$ are chosen uniformly random from $\mathsf{Span}(\mathbf{B})$ in $\mathsf{G}_{3,\hat{\imath},0}$ and uniformly random from $\mathbb{Z}_q^{3k}$ in game $\mathsf{G}_{3,\hat{\imath},1}$. Since for all computed values it is enough to have $[\mathbf{B}]_2$ instead of $\mathbf{B}$ (see Lemma 20 for details), this leads to a straightforward reduction to the $(k+1)Q_e$-fold $\mathcal{U}_{3k,k}$-MDDH assumption. By Lemma 3 this assumption is at most $2k$ times harder then the $\mathcal{U}_{3k,k}$-MDDH assumption, which is equivalent to the $\mathcal{U}_k$-MDDH by Lemma 1.

The running time of $\mathcal{B}$ is dominated by the running time of $\mathcal{A}$ plus some (polynomial) overhead that is independent of $T(\mathcal{A})$ for the group operations in each oracle query. □

Lemma 47 ($\mathsf{G}_{3,\hat{\imath},1} \rightsquigarrow \mathsf{G}_{3,\hat{\imath},3}$)**.** *For all $\hat{\imath} \in \{1, \ldots, L\}$ and all adversaries $\mathcal{A}$ there exist adversaries $\mathcal{B}_1$, $\mathcal{B}_2$ with*

$$\begin{aligned}|\Pr[\mathsf{G}_{3,\hat{\imath},1} \Rightarrow 1] - \Pr[\mathsf{G}_{3,\hat{\imath},3} \Rightarrow 1]| \leq{}& 8k\hat{\imath}\alpha\left(\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},2}(\mathcal{B}_2)\right)\\ &+ k\hat{\imath}\alpha\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}_1) + \frac{(Q_c+6)\hat{\imath}\alpha}{q-1} + \frac{Q_{e,\hat{\imath}}}{q^{k-1}(q-1)}\end{aligned}$$

and $T(\mathcal{B}_1) \approx T(\mathcal{B}_2) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$. $Q_{e,\hat{\imath}}$ denotes the number of Eval *queries with $p = \hat{\imath}$.*

Proof. To prove this transition, we use the hybrids $\mathsf{G}_{3,\hat{\imath},2,\hat{\jmath},0}$ for $\hat{\jmath} \in \{1,\ldots,\hat{\imath}\alpha\}$, $\mathsf{G}_{3,\hat{\imath},2,\hat{\jmath},1}$–$\mathsf{G}_{3,\hat{\imath},2,\hat{\jmath},3}$ for $\hat{\jmath} \in \{1,\ldots,\hat{\imath}\alpha - 1\}$. The hybrids are given in Figure 21.

Lemma 47 follows directly from Lemmata 48–54. □

Lemma 48 ($\mathsf{G}_{3,\hat{\imath},1} \rightsquigarrow \mathsf{G}_{3,\hat{\imath},2,0,0}$)**.**

$$\Pr\left[\mathsf{G}^{\mathcal{A}}_{3,\hat{\imath},1} \Rightarrow 1\right] = \Pr\left[\mathsf{G}^{\mathcal{A}}_{3,\hat{\imath},2,0,0} \Rightarrow 1\right]$$

Proof. The proof is analogous to Lemma 19. □

Lemma 49 ($\mathsf{G}_{3,\hat{\imath},2,\hat{\jmath},0} \rightsquigarrow \mathsf{G}_{3,\hat{\imath},2,\hat{\jmath},1}$)**.** *For $\hat{\jmath} < \hat{\imath}\alpha$ and all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{3,\hat{\imath},2,\hat{\jmath},0} \Rightarrow 1\right] - \Pr\left[\mathsf{G}^{\mathcal{A}}_{3,\hat{\imath},2,\hat{\jmath},1} \Rightarrow 1\right]\right| \leq 4k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},2}(\mathcal{B}) + \frac{2}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. The proof is analogous to Lemma 20, except that we change the distribution of the column vectors of $\mathbf{T}$ additional to the distribution of $\mathbf{t}$. □

Lemma 50 ($\mathsf{G}_{3,\hat{\imath},2,\hat{\jmath},1} \rightsquigarrow \mathsf{G}_{3,\hat{\imath},2,\hat{\jmath},2}$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{3,\hat{\imath},2,\hat{\jmath},1} \Rightarrow 1\right] - \Pr\left[\mathsf{G}^{\mathcal{A}}_{3,\hat{\imath},2,\hat{\jmath},2} \Rightarrow 1\right]\right| \leq k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}) + \frac{Q_c + 2}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. The proof is analogous to Lemma 21. □

Lemma 51 ($\mathsf{G}_{3,\hat{\imath},2,\hat{\jmath},2} \rightsquigarrow \mathsf{G}_{3,\hat{\imath},2,\hat{\jmath},3}$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{3,\hat{\imath},2,\hat{\jmath},2} \Rightarrow 1\right] - \Pr\left[\mathsf{G}^{\mathcal{A}}_{3,\hat{\imath},2,\hat{\jmath},3} \Rightarrow 1\right]\right| \leq k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}) + \frac{Q_c + 2}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. The proof is analogous to Lemma 22. □

Lemma 52 (Optimization: $\mathsf{G}_{3,\hat{\imath},2,\hat{\jmath},1} \rightsquigarrow \mathsf{G}_{3,\hat{\imath},2,\hat{\jmath},3}$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{3,\hat{\imath},2,\hat{\jmath},1} \Rightarrow 1\right] - \Pr\left[\mathsf{G}^{\mathcal{A}}_{3,\hat{\imath},2,\hat{\jmath},3} \Rightarrow 1\right]\right| \leq k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}) + \frac{Q_c + 2}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. The proof is analogous to Lemma 23. □

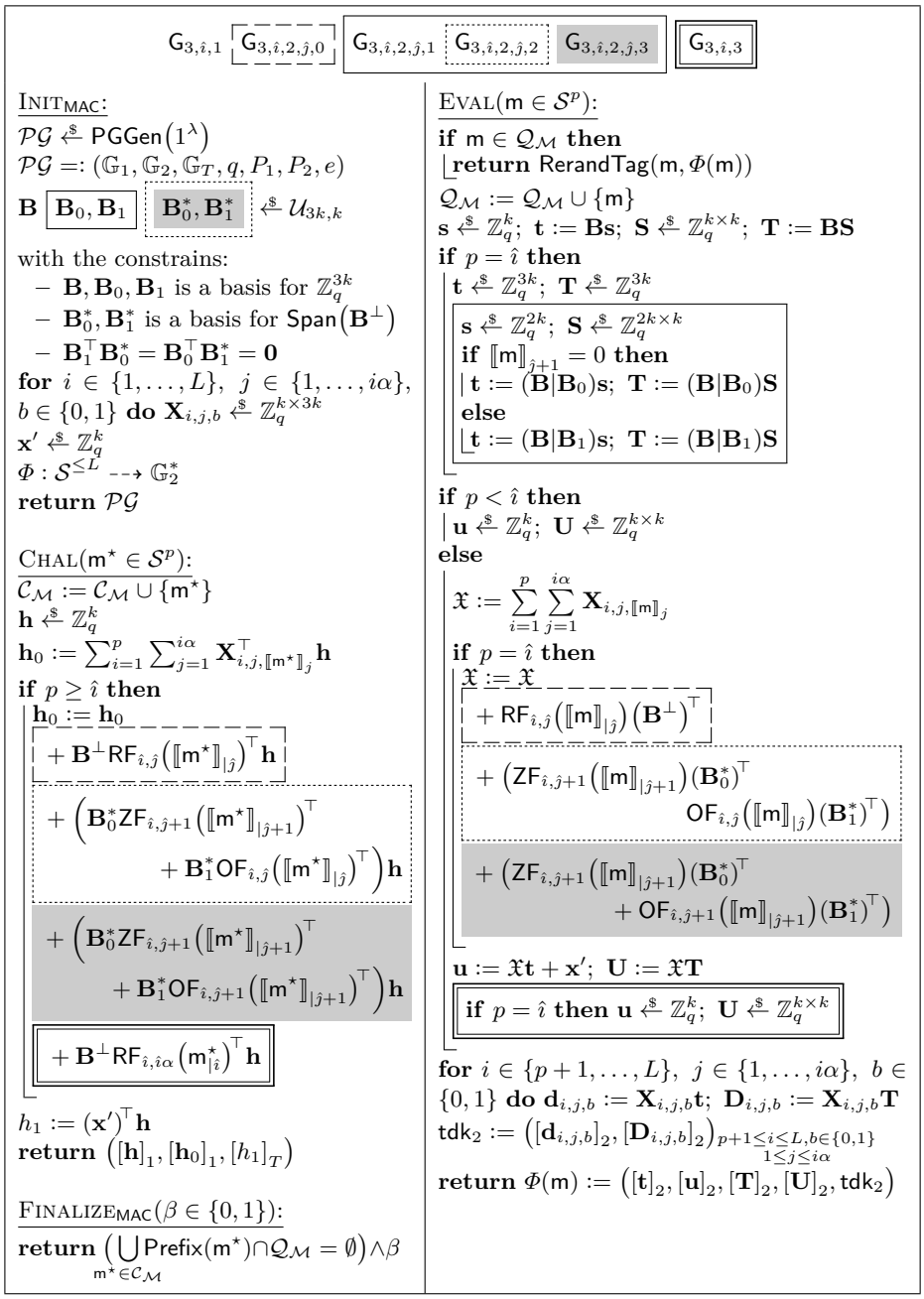


Fig. 21. Hybrids for the transition from $\mathsf{G}_{3,\hat{\imath},1}$ to $\mathsf{G}_{3,\hat{\imath},3}$. The algorithm RerandTag is defined in Figure 20.

Lemma 53 ($\mathsf{G}_{3,\hat{\imath},2,\hat{\jmath},3} \rightsquigarrow \mathsf{G}_{3,\hat{\imath},2,\hat{\jmath}+1,0}$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{3,\hat{\imath},2,\hat{\jmath},3} \Rightarrow 1\right] - \Pr\left[\mathsf{G}^{\mathcal{A}}_{3,\hat{\imath},2,\hat{\jmath}+1,0} \Rightarrow 1\right]\right| \leq 4k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},2}(\mathcal{B}) + \frac{2}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. The proof is analogous to Lemma 24. □

Lemma 54 ($\mathsf{G}_{3,\hat{\imath},2,\hat{\imath}\alpha,0} \rightsquigarrow \mathsf{G}_{3,\hat{\imath},3}$)**.** *Let $Q_{e,\hat{\imath}}$ denote the number of* Eval *queries with $p = \hat{\imath}$.*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{3,\hat{\imath},2,\hat{\imath}\alpha,0} \Rightarrow 1\right] - \Pr\left[\mathsf{G}^{\mathcal{A}}_{3,\hat{\imath},3} \Rightarrow 1\right]\right| \leq \frac{Q_{e,\hat{\imath}}}{q^{k-1}(q-1)}$$

Proof. Assume $\forall \mathsf{m}^\star \in \mathcal{C}_{\mathcal{M}} : \mathsf{Prefix}(\mathsf{m}^\star) \cap \mathcal{Q}_{\mathcal{M}} \neq \emptyset$, otherwise the adversary has lost the game anyway. In each user secret key query with $p = \hat{\imath}$ the value $\mathsf{RF}_{\hat{\imath},\hat{\imath}\alpha}(\mathsf{m})\left(\mathbf{B}^{\perp}\right)^{\top}\mathbf{t}$ is added to u. This is the only place where $\mathsf{RF}_{\hat{\imath},\hat{\imath}\alpha}(\mathsf{m})$ is used, since only the first Eval query for each message evaluates the random function and Chal queries evaluate $\mathsf{RF}_{\hat{\imath},\hat{\imath}\alpha}$ only on prefixes of $\mathsf{m}^\star \in \mathcal{C}_{\mathcal{M}}$.

Furthermore assume, that $\mathbf{t}$ and the column vectors of $\mathbf{T}$ are linear independent and none of them lies in $\mathsf{Span}(\mathbf{B})$. This happens with probability at least $(1 - 1/(q^{k-1}(q-1)))$. In this case each non-duplicated Eval query outputs a uniformly random vector for $\mathbf{U}$ and the games are distributed identically. □

Lemma 55 ($\mathsf{G}_{3,\hat{\imath},3} \rightsquigarrow \mathsf{G}_{3,\hat{\imath},4}$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{3,\hat{\imath},3} \Rightarrow 1\right] - \Pr\left[\mathsf{G}^{\mathcal{A}}_{3,\hat{\imath},4} \Rightarrow 1\right]\right| \leq 2k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}) + \frac{Q_c + 2}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. The proof is analogous to Lemma 26. □

Lemma 56 ($\mathsf{G}_{3,\hat{\imath},4} \rightsquigarrow \mathsf{G}_{3,\hat{\imath},5}$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{3,\hat{\imath},4} \Rightarrow 1\right] - \Pr[\mathsf{G}_{3,\hat{\imath},5} \Rightarrow 1]\right| \leq 2k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},2}(\mathcal{B}) + \frac{1}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. The reduction is the reverse of Lemma 46. □

Lemma 57 ($\mathsf{G}_{3,\hat{\imath},5} \rightsquigarrow \mathsf{G}_{3,\hat{\imath}+1,0}$)**.** *For $\hat{\imath} < L$*

$$\Pr[\mathsf{G}_{3,\hat{\imath},5} \Rightarrow 1] = \Pr[\mathsf{G}_{3,\hat{\imath}+1,0} \Rightarrow 1].$$

Proof. These two games are equivalent. □

$\underline{\text{INIT}_{\mathsf{MAC}}}$:
$\mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
$\mathbf{B} \xleftarrow{\$} \mathcal{U}_{3k,k}$
for $i \in \{1, \dots, L\},\ j \in \{1, \dots, i\alpha\},\ b \in \{0,1\}$ **do**
  $\mathbf{J}_{i,j,b} \xleftarrow{\$} \mathbb{Z}_q^{k \times 3k}$
  if $(i,j) \neq (1,1)$ **then** $\mathbf{X}_{i,j,b} := \mathbf{J}_{i,j,b}$
// Implicit: For $b \in \{0,1\}$:
// $\mathbf{X}_{1,1,b} := \mathbf{J}_{1,1,b} + \overline{\mathbf{D}}^{-\top}\underline{\mathbf{D}}^{\top}$
$\mathbf{x}' \xleftarrow{\$} \mathbb{Z}_q^k$
$\Phi : \mathcal{S}^{\leq L} \dashrightarrow \mathbb{G}_2^*$
return $\mathcal{PG}$

$\underline{\text{FINALIZE}_{\mathsf{MAC}}(\beta \in \{0,1\})}$:
return $\left(\bigcup_{\mathsf{m}^\star \in \mathcal{C}_\mathcal{M}} \mathsf{Prefix}(\mathsf{m}^\star) \cap \mathcal{Q}_\mathcal{M} = \emptyset\right) \wedge \beta$

$\underline{\text{EVAL}(\mathsf{m} \in \mathcal{S}^p)}$:
if $\mathsf{m} \in \mathcal{Q}_\mathcal{M}$ **then**
  return $\mathsf{RerandTag}(\mathsf{m}, \Phi(\mathsf{m}))$
$\mathcal{Q}_\mathcal{M} := \mathcal{Q}_\mathcal{M} \cup \{\mathsf{m}\}$
$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k;\ \mathbf{t} := \mathbf{Bs};\ \mathbf{S} \xleftarrow{\$} \mathbb{Z}_q^{k \times k};\ \mathbf{T} := \mathbf{BS}$
$\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^k;\ \mathbf{U} \xleftarrow{\$} \mathbb{Z}_q^{k \times k}$
for $i \in \{p+1, \dots, L\},\ j \in \{1, \dots, i\alpha\},\ b \in \{0,1\}$ **do** $\mathbf{d}_{i,j,b} := \mathbf{X}_{i,j,b}\mathbf{t};\ \mathbf{D}_{i,j,b} := \mathbf{X}_{i,j,b}\mathbf{T}$
$\mathsf{tdk}_2 := \left([\mathbf{d}_{i,j,b}]_2, [\mathbf{D}_{i,j,b}]_2\right)_{\substack{p+1 \leq i \leq L, b \in \{0,1\} \\ 1 \leq j \leq i\alpha}}$
return $\Phi(\mathsf{m}) := \left([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{T}]_2, [\mathbf{U}]_2, \mathsf{tdk}_2\right)$

$\underline{\text{CHAL}(\mathsf{m}^\star \in \mathcal{S}^p)}$:
$\mathcal{C}_\mathcal{M} := \mathcal{C}_\mathcal{M} \cup \{\mathsf{m}^\star\}$
Let this be the c-th CHAL query.
$\mathbf{h} := \overline{\mathbf{f}_c}$
$\mathbf{h}_0 := \sum_{i=1}^{p} \sum_{j=1}^{i\alpha} \mathbf{J}_{i,j,[\![\mathsf{m}^\star]\!]_j}^{\top} \mathbf{h} + \underline{\mathbf{f}_c}$
$h_1 := (\mathbf{x}')^{\top}\mathbf{h}$
return $\left([\mathbf{h}]_1, [\mathbf{h}_0]_1, [h_1]_T\right)$

Fig. 22. Reduction for the transition from $\mathsf{G}_{3,L,5}$ to G_4 to the Q_c-fold $\mathcal{U}_{2k,k}$ challenge $\left([\mathbf{D}]_1, [\mathbf{f}_1]_1, \dots, [\mathbf{f}_{Q_c}]_1\right)$.

Lemma 58 ($\mathsf{G}_{3,L,5} \rightsquigarrow \mathsf{G}_4$)**.**

$$\left|\Pr[\mathsf{G}_{3,L,5} \Rightarrow 1] - \Pr\left[\mathsf{G}_4^{\mathcal{A}} \Rightarrow 1\right]\right| \leq 3k\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}) + \frac{2}{q-1}$$

Proof. To bound the difference between these two games, pick a Q_c-fold $\mathcal{U}_{4k,k}$-MDDH challenge $\left([\mathbf{D}]_1, [\mathbf{f}_1]_1, \dots, [\mathbf{f}_{Q_c}]_1\right)$ and use the reduction given in Figure 22.

INIT and EVAL are identical in game $\mathsf{G}_{3,L,5}$ and G_4. EVAL is simulated correctly by the reduction because $\mathbf{X}_{1,1,0}$ and $\mathbf{X}_{1,1,1}$ are not used there.

Assume that $\overline{\mathbf{D}}$ is invertible. This happens with probability at least $(1 - 1/(q-1))$. To analyze the CHAL queries write $\mathbf{f}_c =: \begin{pmatrix} \overline{\mathbf{D}}\mathbf{w}_c \\ \underline{\mathbf{D}}\mathbf{w}_c + \mathbf{r}_c \end{pmatrix}$ where $\mathbf{w}_c$ is uniform random in $\mathbb{Z}_q^k$ and $\mathbf{r}_c$ is $\mathbf{0} \in \mathbb{Z}_q^{3k}$ or uniform random in $\mathbb{Z}_q^{3k}$. Then $\mathbf{h} := \overline{\mathbf{f}_c}$ is a uniform random vector in $\mathbb{Z}_q^k$, since $\overline{\mathbf{D}}$ has full rank and $\mathbf{w}_c$ is uniformly random.

The value $\mathbf{h}_0$ is calculated as

$$\begin{aligned}\mathbf{h}_0 &:= \sum_{i=1}^{p} \sum_{j=1}^{i\alpha} \mathbf{J}_{i,j,[\![\mathsf{m}^\star]\!]_j}^{\top} \mathbf{h} + \underline{\mathbf{f}_c} = \sum_{i=1}^{p} \sum_{j=1}^{i\alpha} \mathbf{J}_{i,j,[\![\mathsf{m}^\star]\!]_j}^{\top} \mathbf{h} + \underline{\mathbf{D}}\overline{\mathbf{D}}^{-1}\overline{\mathbf{f}_c} + \mathbf{r}_c \\ &= \sum_{i=1}^{p} \sum_{j=1}^{i\alpha} \mathbf{X}_{i,j,[\![\mathsf{m}^\star]\!]_j}^{\top} \mathbf{h} + \mathbf{r}_c\,.\end{aligned}$$

If $\mathbf{r}_c = \mathbf{0}$, we are simulating game $\mathsf{G}_{3,L,5}$. If $\mathbf{r}_c$ is uniform random, then $\mathbf{h}_0$ is uniform random and we are simulating game G_4. □

Lemma 59 ($\mathsf{G}_4 \rightsquigarrow \mathsf{G}_5$)**.**

$$\left|\Pr\left[\mathsf{G}_4^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_5^{\mathcal{A}} \Rightarrow 1\right]\right| \leq \mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{PGGen},1}(\mathcal{B}) + \frac{2}{q-1}$$

Proof. The proof is analogous to Lemma 29. □

Summary. To prove Theorem 4, we combine Lemmata 43–59 to change $\mathbf{h}_0$ and h_1 from real to random and then apply Lemmata 57–43 in reverse order to get to the $\mathsf{mAPR\text{-}CMA}_{\mathsf{rand}}$ game. The Lemmata 50 and 51 resp. Lemma 52 get information theoretic arguments then. □

D Transformation to standard HIBE

D.1 Hierarchical Identity-based Key Encapsulation

We recall syntax and security of a hierarchical identity-based key encapsulation mechanism (HIBKEM). We only consider HIBKEM in this paper. By adapting the transformation for public-key encryption in [26] to the HIBE setting, one can easily prove that every HIBKEM can be transformed (tightly) into an HIBE scheme with a (one-time secure) symmetric cipher.

Definition 9 (Hierarchical identity-based key encapsulation mechanism). *A* hierarchical identity-based key encapsulation mechanism *(HIBKEM)* HIBKEM *consists of five polynomial-time algorithms* $\mathsf{HIBKEM} := (\mathsf{Gen}, \mathsf{Del}, \mathsf{Ext}, \mathsf{Enc}, \mathsf{Dec})$ *with the following properties.*

- *The probabilistic key generation algorithm* $\mathsf{Gen}(1^\lambda)$ *returns the (master) public/delegation/secret key* $(\mathsf{pk}, \mathsf{dk}, \mathsf{sk})$*. Note that for some of the constructions in this paper* dk *is empty. We assume that* pk *implicitly defines a hierarchical identity space* $\mathcal{ID} = \mathcal{S}^{\leq L}$*, for some base identity set* $\mathcal{S}$*, a user secret key space* $\mathcal{USK}$ *a key space* $\mathcal{K}$ *and a ciphertext space* $\mathcal{C}$*.*
- *The probabilistic user secret key generation algorithm* $\mathsf{Ext}(\mathsf{sk}, \mathsf{id})$ *returns a secret key* $\mathsf{usk}[\mathsf{id}]$ *and a delegation key* $\mathsf{udk}[\mathsf{id}]$ *for a hierarchical identity* $\mathsf{id} \in \mathcal{ID}$*. Note that for some of the constructions in this paper* $\mathsf{udk}[\mathsf{id}]$ *is empty.*
- *The probabilistic key delegation algorithm* $\mathsf{Del}(\mathsf{dk}, \mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}], \mathsf{id} \in \mathcal{S}^p, \mathsf{id}_{p+1} \in \mathcal{S})$ *returns a user secret key* $\mathsf{usk}[\mathsf{id}|\mathsf{id}_{p+1}]$ *for the hierarchical identity* $\mathsf{id}' = \mathsf{id} \mid \mathsf{id}_{p+1} \in \mathcal{S}^{p+1}$ *and the user delegation key* $\mathsf{udk}[\mathsf{id}']$*. We require* $1 \leq |\mathsf{id}| \leq L - 1$*.*
- *The probabilistic encapsulation algorithm* $\mathsf{Enc}(\mathsf{pk}, \mathsf{id})$ *returns a symmetric key* $\mathsf{K} \in \mathcal{K}$ *together with a ciphertext* C *with respect to the hierarchical identity* $\mathsf{id} \in \mathcal{ID}$*.*
- *The deterministic decapsulation algorithm* $\mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id}, \mathsf{C})$ *returns a decapsulated key* $\mathsf{K} \in \mathcal{K}$ *or the reject symbol* $\perp$*.*

INIT: $(\mathsf{pk}, \mathsf{dk}, \mathsf{sk}) \xleftarrow{\$} \mathsf{Gen}(\lambda)$ **return** $(\mathsf{pk}, \mathsf{dk})$ EXT(id): $\mathcal{Q}_{\mathcal{ID}} \leftarrow \mathcal{Q}_{\mathcal{ID}} \cup \{\mathsf{id}\}$ **return** $(\mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}]) \xleftarrow{\$} \mathsf{Ext}(\mathsf{sk}, \mathsf{id})$	ENC($\mathsf{id}^\star$): $\mathcal{C}_{\mathcal{ID}} := \mathcal{C}_{\mathcal{ID}} \cup \{\mathsf{id}^\star\}$ $(\mathsf{K}^\star, \mathsf{C}^\star) \xleftarrow{\$} \mathsf{Enc}(\mathsf{pk}, \mathsf{id}^\star)$ $\boxed{\mathsf{K}^\star \xleftarrow{\$} \mathcal{K}}$ $(\mathsf{K}^\star, \mathsf{C}^\star) \xleftarrow{\$} \mathcal{K} \times \mathcal{C}$ **return** $(\mathsf{K}^\star, \mathsf{C}^\star)$ FINALIZE($\beta \in \{0,1\}$): **return** $\Big(\bigcup_{\mathsf{id}^\star \in \mathcal{C}_{\mathcal{ID}}} \mathsf{Prefix}(\mathsf{id}^\star) \cap \mathcal{Q}_{\mathcal{ID}} = \emptyset\Big) \wedge \beta$

Fig. 23. Games $\mathsf{mIND\text{-}HID\text{-}CPA}_{\mathsf{real}}$, $\boxed{\mathsf{mIND\text{-}HID\text{-}CPA}_{\mathsf{rand}}}$, and $\mathsf{mPR\text{-}HID\text{-}CPA}_{\mathsf{rand}}$ for defining mIND-HID-CPA and mPR-HID-CPA security. For any identity $\mathsf{id} \in \mathcal{S}^p$, $\mathsf{Prefix}(\mathsf{id})$ denotes the set of all prefixes of id.

We make the delegation key dk explicit to make the constructions in this paper more readable. We define indistinguishability (IND-HID-CPA) against adaptively chosen identity and plaintext attacks for a HIBKEM via games $\mathsf{IND\text{-}HID\text{-}CPA}_{\mathsf{real}}$ and $\mathsf{IND\text{-}HID\text{-}CPA}_{\mathsf{rand}}$ from Figure 23.

Definition 10 (Delegation Invariance). *An HIBKEM* $\mathsf{HIBKEM} := (\mathsf{Gen}, \mathsf{Del}, \mathsf{Ext}, \mathsf{Enc}, \mathsf{Dec})$ *is* delegation invariant*, if the distribution of* $\mathsf{usk}[\mathsf{id}|\mathsf{id}_{p+1}]$ *generated by* $\mathsf{Del}(\mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}], \mathsf{id}, \mathsf{id}_{p+1})$ *for any valid user secret key* $\mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}]$ *for* id *is independent of* $\mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}]$ *and identical to the distribution of keys generated by* $\mathsf{Ext}(\mathsf{sk}, \mathsf{id}|\mathsf{id}_{p+1})$*.*

In this paper, we focus only on HIBKEM schemes with delegation invariance. The following definitions of correctness and security are only suitable for delegation invariant schemes. For general HIBKEMs, a more involved definition that takes the Del algorithm into account is necessary (see [40]).

Definition 11 (Correctness). *A delegation invariant HIBKEM* $\mathsf{HIBKEM} := (\mathsf{Gen}, \mathsf{Del}, \mathsf{Ext}, \mathsf{Enc}, \mathsf{Dec})$ *is* correct*, if for all* $\lambda \in \mathbb{N}_+$*, all pairs* $(\mathsf{pk}, \mathsf{sk})$ *generated by* $\mathsf{Gen}(\lambda)$*, all* $\mathsf{id} \in \mathcal{ID}$*, all* $\mathsf{usk}[\mathsf{id}]$ *generated by* $\mathsf{Ext}(\mathsf{sk}, \mathsf{id})$ *and all* (K, c) *generated by* $\mathsf{Enc}(\mathsf{pk}, \mathsf{id})$*:*

$$\Pr[\mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id}, \mathsf{C}) = \mathsf{K}] = 1.$$

An IBKEM is an HIBKEM with $L = 1$. The algorithm Del and the keys dk and $\mathsf{udk}[\mathsf{id}]$ are unnecessary in this case.

We consider two different security notions for HIBKEMs in this work. The first one is indistinguishability under chosen plaintext attacks, the standard notion (here in the multi-challenge setting) that guarantees that the encapsulated key is hidden from the adversary.

Definition 12 (mIND-HID-CPA Security). *A delegation invariant hierarchical identity-based key encapsulation scheme* HIBKEM *is* mIND-HID-CPA-secure *if for all PPT adversaries* $\mathcal{A}$*,*

$$\mathsf{Adv}^{\text{mind-hid-cpa}}_{\mathsf{HIBKEM},\mathsf{PGGen}}(\mathcal{A}) := |\Pr[\text{mIND-HID-CPA}^{\mathcal{A}}_{\mathsf{real}} \Rightarrow 1] - \Pr[\text{mIND-HID-CPA}^{\mathcal{A}}_{\mathsf{rand}}]|$$

is negligible. The games $\text{mIND-HID-CPA}_{\mathsf{real}}$ *and* $\text{mIND-HID-CPA}_{\mathsf{rand}}$ *are defined in Figure 23.*

The second notion we consider here is pseudorandomness under chosen-plaintext attacks. This notion also guarantees the pseudorandomness of the challenge ciphertexts and thus implies anonymity, i.e., the adversary can not distinguish ciphertexts encrypted under different identities, when he has not queried a user secret key for one of the identities.

Definition 13 (mPR-HID-CPA Security). *A delegation invariant hierarchical identity-based key encapsulation scheme* HIBKEM *is* mPR-HID-CPA-secure *if for all PPT adversaries* $\mathcal{A}$*,*

$$\mathsf{Adv}^{\text{pr-hid-cpa}}_{\mathsf{HIBKEM}}(\mathcal{A}) := |\Pr[\text{mIND-HID-CPA}^{\mathcal{A}}_{\mathsf{real}} \Rightarrow 1] - \Pr[\text{mPR-HID-CPA}^{\mathcal{A}}_{\mathsf{rand}} \Rightarrow 1]|$$

is negligible. The games $\text{mIND-HID-CPA}_{\mathsf{real}}$ *and* $\text{mPR-HID-CPA}_{\mathsf{rand}}$ *are defined in Figure 23.*

For an IBKEM this security notion is called mPR-CPA.

D.2 CPA-secure Transformation

Any affine MAC with levels can be transformed tightly to an IND-HID-CPA-secure hierarchical identity-based key encapsulation mechanism (HIBKEM) under the $\mathcal{D}_{k+\eta,k}$-MDDH assumption in $\mathbb{G}_1$. The transformation is shown in Figure 10. It is identical to the one in [32], except that we consider multi-challenge security here.

Theorem 5 (Delegation Invariance). *For an affine MAC with levels* MAC*, the HIBKEM* $\mathsf{HIBKEM}_{\mathsf{CPA}}[\mathsf{MAC}, \mathcal{D}_{k+\eta,k}]$ *is delegation invariant.*

Proof. The user secret keys outputted by the Del algorithm are valid user secret keys with randomness $(\mathbf{t}'_l)_{1\leq l\leq \ell(p)}$ where $\mathbf{t}_l := \mathbf{t}_l + \mathbf{B}\mathbf{s}'_l$ for $l \in \{1,\ldots,p\}$. Since $\mathbf{s}'_l$ is a fresh uniform random vector and $\mathbf{t}_l \in \mathsf{Span}(\mathbf{B})$, $\mathbf{t}'_l$ is a fresh random vector from $\mathsf{Span}(\mathbf{B})$. Thus a delegated user secret key is distributed like an user secret key generated with the Ext algorithm. □

Theorem 6 (Correctness). *The HIBKEM* $\mathsf{HIBKEM}_{\mathsf{CPA}}[\mathsf{MAC}, \mathcal{D}_{k+\eta,k}]$ *is correct.*

Proof. The Dec algorithm returns – when used with a user secret key for the identity used for encryption – $[\mathsf{K}]_T$ with

$$\begin{aligned}\mathsf{K} &:= \mathbf{c}_0^\top \begin{pmatrix}\mathbf{v}\\ \mathbf{u}\end{pmatrix} - \sum_{l=1}^{\ell(p)} \mathbf{c}_{1,l}^\top \mathbf{t}_l \\ &= \mathbf{r}^\top \mathbf{A}^\top \left(\sum_{l=1}^{\ell(p)} \sum_{i=1}^{p} \sum_{j=1}^{\ell'(l,i)} f_{l,i,j}\big(\mathsf{id}_{|i}\big) \begin{pmatrix}\mathbf{Y}_{l,i,j}\\ \mathbf{X}l,i,j\end{pmatrix} \mathbf{t}_l + \begin{pmatrix}\mathbf{y}'\\ \mathbf{x}'\end{pmatrix} \right) \\ &\quad - \sum_{l=1}^{\ell(p)} \left(\sum_{i=1}^{p} \sum_{j=1}^{\ell'(l,i)} f_{l,i,j}\big(\mathsf{id}_{|i}\big) \mathbf{Z}_{l,i,j}\mathbf{r} \right)^\top \mathbf{t}_l \\ &= \mathbf{r}^\top \mathbf{A}^\top \begin{pmatrix}\mathbf{y}'\\ \mathbf{x}'\end{pmatrix} = \mathbf{z}'\mathbf{r}\,,\end{aligned}$$

which is the key the Enc algorithm returned as well. □

Theorem 7 (Security). *The HIBKEM* $\mathsf{HIBKEM}_{\mathsf{CPA}}[\mathsf{MAC}, \mathcal{D}_{k+\eta,k}]$ *is* mIND-HID-CPA *secure under the* $\mathcal{D}_{k+\eta,k}$-MDDH *assumption for* $\mathbb{G}_1$ *if* MAC *is* mHPR-CMA *secure. More precisely, for all adversaries* $\mathcal{A}$ *there exist adversaries* $\mathcal{B}_1$ *and* $\mathcal{B}_2$ *with*

$$\begin{aligned}\mathsf{Adv}^{\mathsf{mind\text{-}hid\text{-}cpa}}_{\mathsf{HIBKEM}_{\mathsf{CPA}}[\mathsf{MAC},\mathcal{D}_{k+\eta,k}],\mathsf{PGGen}}(\mathcal{A}) &\le \mathsf{Adv}^{\mathsf{mhpr\text{-}cma}}_{\mathsf{MAC},\mathsf{PGGen}}(\mathcal{B}_1) \\ &\quad + 2\eta \mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{D}_{k+\eta,k},\mathsf{PGGen},1}(\mathcal{B}_2) + \frac{4}{q-1}\end{aligned}$$

and $T(\mathcal{B}_1) \approx T(\mathcal{B}_2) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$*, where* Q_e *resp.* Q_c *denotes the number of* Eval *resp.* Chal *queries of* $\mathcal{A}$ *and* poly *is a polynomial independent of* $\mathcal{A}$*.*

Proof. The proof makes use of the hybrids G_0–G_4 defined in Figure 24. G_0 is the $\mathsf{mIND\text{-}HID\text{-}CPA}_{\mathsf{real}}$ game.

Lemma 60 ($\mathsf{G}_0 \rightsquigarrow \mathsf{G}_1$)**.**

$$\Pr\big[\mathsf{G}_0^{\mathcal{A}} \Rightarrow 1\big] = \Pr\big[\mathsf{G}_1^{\mathcal{A}} \Rightarrow 1\big]$$

Proof. The only difference between these games is that $\mathbf{c}^\star_{1,l}$ and $\mathsf{K}^\star$ are computed with the public value $\mathbf{Z}_{l,i,j}$ in game G_0 and with the secret key $\mathbf{X}_{l,i,j}$ and $\mathbf{Y}_{l,i,j}$ in G_1. □

Lemma 61 ($\mathsf{G}_1 \rightsquigarrow \mathsf{G}_2$)**.** *For all adversaries* $\mathcal{A}$ *there exists an adversary* $\mathcal{B}$ *with*

$$\big|\Pr\big[\mathsf{G}_1^{\mathcal{A}} \Rightarrow 1\big] - \Pr\big[\mathsf{G}_2^{\mathcal{A}} \Rightarrow 1\big]\big| \le \eta \mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{D}_{k+\eta,k},\mathsf{PGGen},1}(\mathcal{B}) + \frac{1}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$*.*

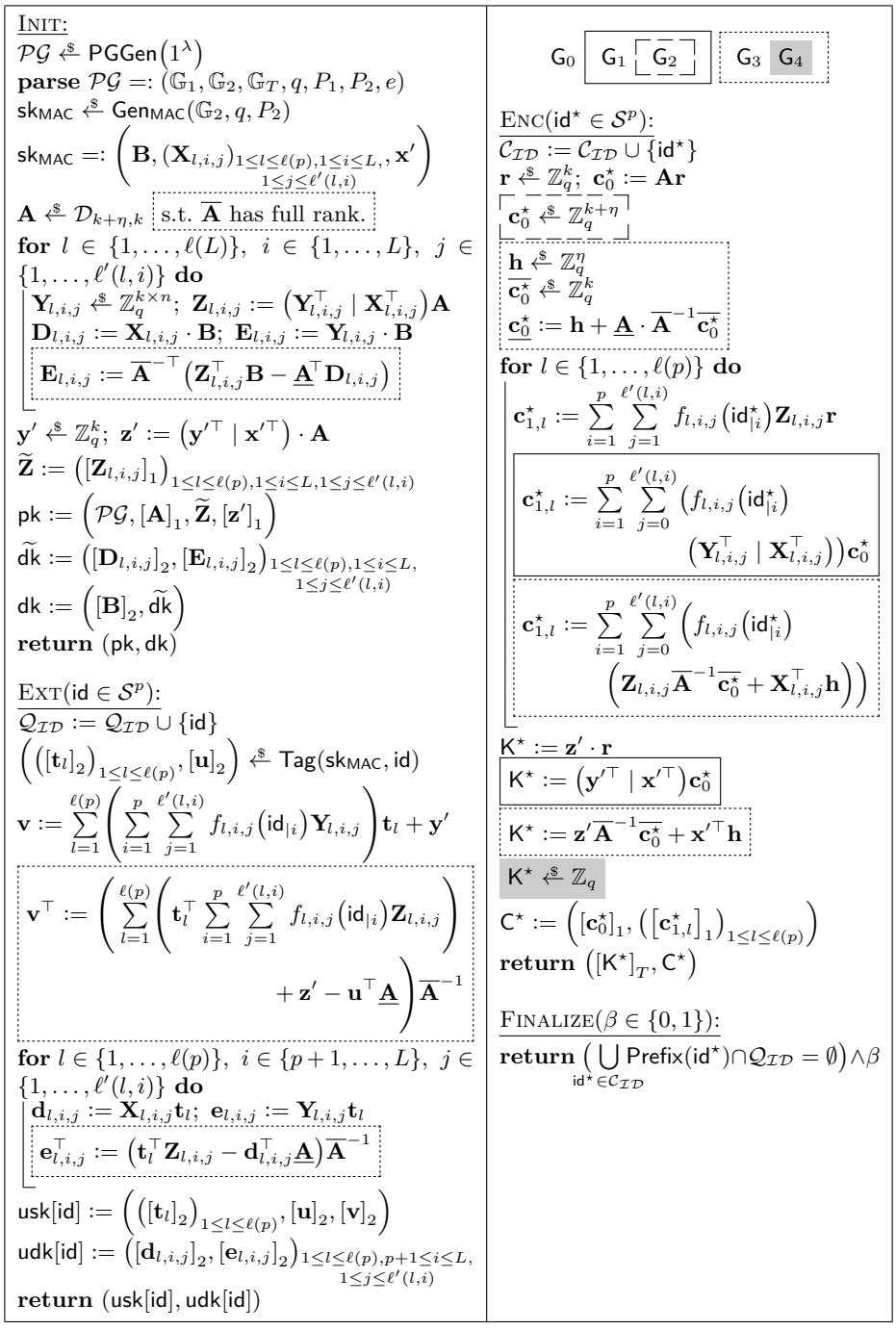


Fig. 24. Hybrids for the security proof of the $\mathsf{HIBKEM}_{\mathsf{CPA}}$ transformation.

Proof. The only difference between these games is that $\mathbf{c}_0^\star$ is chosen from $\mathsf{Span}(\mathbf{A})$ in G_1 and from $\mathbb{Z}_q^{k+\eta}$ in G_2. This leads to a straightforward reduction to the Q_c-fold $\mathcal{D}_{k+\eta,k}$-MDDH assumption, where Q_c denotes the number of challenge queries.

The running time of $\mathcal{B}$ is dominated by the running time of $\mathcal{A}$ plus some (polynomial) overhead that is independent of $T(\mathcal{A})$ for the group operations in each oracle query. □

Lemma 62 ($\mathsf{G}_2 \rightsquigarrow \mathsf{G}_3$)**.**

$$\left|\Pr\left[\mathsf{G}_2^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_3^{\mathcal{A}} \Rightarrow 1\right]\right| \leq \frac{1}{q-1}$$

Proof. We assume from now on that $\overline{\mathbf{A}}$ has full rank. This happens with probability at least $(1 - 1/(q-1))$. Next notice that the values $\mathbf{Z}_{l,i,j}$ and $\mathbf{z}'$ are uniform random when $\mathbf{Y}_{l,i,j}$ and $\mathbf{y}'$ are hidden, so $\mathbf{Z}_{l,i,j}$ and $\mathbf{z}'$ are distributed identical in both games. Second notice

$$\mathbf{Z}_{l,i,j} := \left(\mathbf{Y}_{l,i,j}^\top \mid \mathbf{X}_{l,i,j}^\top\right) \cdot \mathbf{A} \iff \mathbf{Y}_{l,i,j}^\top = \left(\mathbf{Z}_{l,i,j} - \mathbf{X}_{l,i,j}^\top \underline{\mathbf{A}}\right)\overline{\mathbf{A}}^{-1}$$

and similarly

$$\mathbf{z}' := \left(\mathbf{y}'^\top \mid \mathbf{x}'^\top\right) \cdot \mathbf{A} \iff \mathbf{y}'^\top = \left(\mathbf{z}' - \mathbf{x}'^\top \underline{\mathbf{A}}\right)\overline{\mathbf{A}}^{-1}.$$

Game G_3 is obtained from G_2 by choosing $\mathbf{Z}_{l,i,j}$ and $\mathbf{z}'$ uniform random and replacing all occurrences of the values $\mathbf{Y}_{l,i,j}$ and $\mathbf{y}'$ by the terms described by the above equations. Thus the games are almost equally distributed. □

Lemma 63 ($\mathsf{G}_3 \rightsquigarrow \mathsf{G}_4$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}_3^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_4^{\mathcal{A}} \Rightarrow 1\right]\right| \leq \mathsf{Adv}^{\mathsf{mhpr\text{-}cma}}_{\mathsf{MAC},\mathsf{PGGen}}(\mathcal{B})$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. The adversary $\mathcal{B}$ is given in Figure 25. When $\mathcal{B}$ plays the $\mathsf{mHPR\text{-}CMA}_{\mathsf{real}}$ game with the affine MAC with levels challenger, he simulates the game G_3 for $\mathcal{A}$. On the other hand, when $\mathcal{B}$ plays the $\mathsf{mHPR\text{-}CMA}_{\mathsf{rand}}$ game with the MAC challenger, he simulates the game G_4 for $\mathcal{A}$.

The running time of $\mathcal{B}$ is dominated by the running time of $\mathcal{A}$ plus some (polynomial) overhead that is independent of $T(\mathcal{A})$ for the group operations in each oracle query. □

Summary. To prove Theorem 7, we combine Lemmata 60–63 to change the challenge keys $\mathsf{K}^\star$ from real to random and then apply all Lemmata (except Lemma 63) in reverse order to get to the $\mathsf{mIND\text{-}HID\text{-}CPA}_{\mathsf{rand}}$ game. □

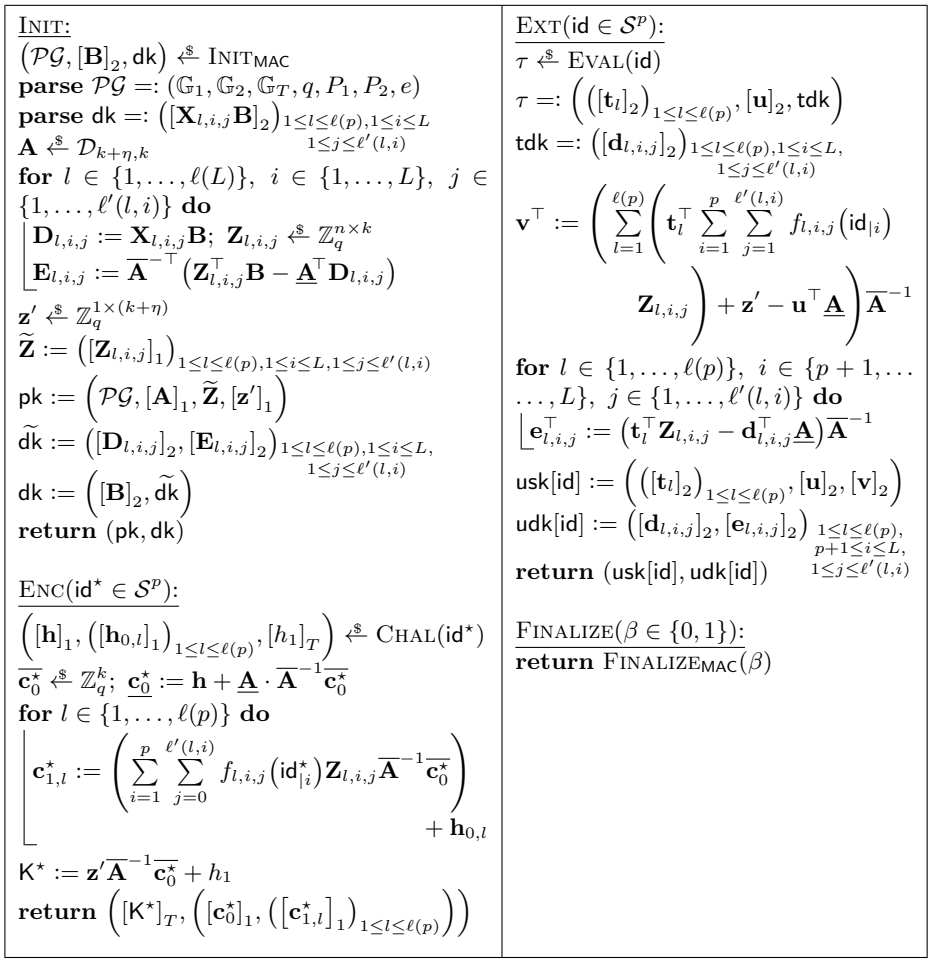


Fig. 25. Adversary $\mathcal{B}$ for Lemma 63.

D.3 CCA-secure Transformation

The transformation from the previous section gives us an HIBE that is only IND-HID-CPA-secure. However, the stronger IND-HID-CCA security notion, that gives an adversary access to a decryption oracle, is more realistic.

An IND-HID-CPA-secure HIBE can be transformed tightly in an IND-HID-CCA-secure one with the CHK-transformation [9] using a strong[5] one-time secure signature: Therefore the identity space of the IND-HID-CPA-secure HIBE is splitted into to distinct parts: The new identity space of the IND-HID-CCA-secure HIBE and the verification key space of the signature scheme. To encrypt a message m for id one generates a signing and verification key pair $(\mathsf{sk}, \mathsf{vk})$. The message m is then encrypted for the identity $\mathsf{id}||\mathsf{vk}$ and signed with sk. The ciphertext is equipped with the signature and vk. To decrypt, one verfies the signature with vk and – if the signature was correct — decrypts the actual ciphertext.

The reduction can now simulate the decryption oracle, because when the ciphertext uses a new verification key, i.e. a verification key vk that has not been used for the identity id before, the reduction can ask for $\mathsf{usk}[\mathsf{id}||\mathsf{vk}]$ and decrypt with this key. Even when id turns (later) out to be the challenge identity, it is unproblematic to query for $\mathsf{usk}[\mathsf{id}||\mathsf{vk}]$. If vk is not new, i.e. vk was generated in a challenge query for id during the reduction, the adversary must have forged a signature (assuming the queried ciphertext is not one of the challenge ciphertexts, in this case the decryption query would be invalid).

The CHK transformation is tightly secure in the single-challenge setting. In the multi-challenge setting it is also tightly secure, if the signature scheme used is tightly secure in the multi-instance setting.

Another approach is to construct a IND-HID-CCA-secure HIBE directly. With an unbounded simulation-sound (USS) tag-based quasi-adaptive non-interactive zero-knowledge argument (QANIZK) [29] for linear subspaces we can transform an affine MAC with levels directly to an constrained chosen-ciphertext (IND-HID-CCCA) secure HIBEKEM. This has been represented in [25] for IBEs, but it works likewise for HIBEs. IND-HID-CCCA-secure HIBEKEMs can be transformed to IND-HID-CCA-secure HIBEs with a (one-time secure) *authenticated* symmetric cipher by adapting a similar transformation for public-key encryption in [26].

Definition 14 (IND-HID-CCCA security). *An HIBKEM* HIBKEM *is* IND-HID-CCCA-secure *in* $\mathbb{G}_2$ *if for all PPT adversaries* $\mathcal{A}$ *where*

$$\mathsf{uncert}(\mathcal{A}) := \frac{1}{Q_d} \sum_{i=1}^{Q_d} \Pr_{\mathsf{K} \in \mathcal{K}}[\mathsf{pred}_i(\mathsf{K}) = 1]$$

is negligible in λ*, the function*

$$\mathsf{Adv}^{\mathsf{mind\text{-}hid\text{-}ccca}}_{\mathsf{HIBKEM}}(\mathcal{A}) := \Big| \Pr\Big[\mathsf{IND\text{-}HID\text{-}CCCA}^{\mathcal{A}}_{\mathsf{real}} \Rightarrow 1\Big] - \Pr\Big[\mathsf{IND\text{-}HID\text{-}CCCA}^{\mathcal{A}}_{\mathsf{rand}} \Rightarrow 1\Big]\Big|$$

[5] A signature is *strong* if it is infeasible to generate a new signature for a message m, even when other signatures for m are known.

INIT:
$(\mathsf{pk}, \mathsf{dk}, \mathsf{sk}) \xleftarrow{\$} \mathsf{Gen}(\lambda)$
return $(\mathsf{pk}, \mathsf{dk})$
 	
EXT(id):
$\mathcal{Q}_{\mathcal{ID}} \leftarrow \mathcal{Q}_{\mathcal{ID}} \cup \{\mathsf{id}\}$
return $(\mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}]) \xleftarrow{\$} \mathsf{Ext}(\mathsf{sk}, \mathsf{id})$
 	
ENC($\mathsf{id}^\star$):
$(\mathsf{K}^\star, \mathsf{C}^\star) \xleftarrow{\$} \mathsf{Enc}(\mathsf{pk}, \mathsf{id}^\star)$
$\mathcal{C}_{\mathsf{enc}} := \mathcal{C}_{\mathsf{enc}} \cup \{(\mathsf{id}^\star, \mathsf{C}^\star)\}$
$\boxed{\mathsf{K}^\star \xleftarrow{\$} \mathcal{K}}$
return $(\mathsf{K}^\star, \mathsf{C}^\star)$
	DEC($\mathsf{id} \in \mathcal{S}^p, \mathsf{C}, \mathsf{pred}$):
	$(\mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}]) \xleftarrow{\$} \mathsf{Ext}(\mathsf{sk}, \mathsf{id})$
	$\mathsf{K} \xleftarrow{\$} \mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id}, \mathsf{C})$
	if $(\mathsf{id}, \mathsf{C}) \notin \mathcal{C}_{\mathsf{enc}} \wedge \mathsf{pred}(\mathsf{K}) = 1$ **then**
	$\quad$ **return** K
	else
	$\quad$ **return** $\perp$
	
	FINALIZE($\beta \in \{0,1\}$):
	return $\Big(\bigcup_{(\mathsf{id}^\star, \mathsf{C}^\star) \in \mathcal{C}_{\mathsf{enc}}} \mathsf{Prefix}(\mathsf{id}^\star) \cap \mathcal{Q}_{\mathcal{ID}} = \emptyset \Big) \wedge \beta$

Fig. 26. Games $\mathsf{IND\text{-}HID\text{-}CCCA}_{\mathsf{real}}$ and $\boxed{\mathsf{IND\text{-}HID\text{-}CCCA}_{\mathsf{rand}}}$ for defining IND-HID-CCCA security. In DEC the time need for evaluating the polynomial-time algorithm pred is charged to the adversaries run time.

is negligible as well. The games $\mathsf{IND\text{-}HID\text{-}CCCA}_{\mathsf{real}}$ *and* $\mathsf{IND\text{-}HID\text{-}CCCA}_{\mathsf{rand}}$ *are defined in Figure 26. The number of* DEC *queries of* $\mathcal{A}$ *is denoted by* Q_d *and* pred_i $(1 \leq i \leq Q_d)$ *is the* pred *algorithm of the* i*-th* DEC *query of* $\mathcal{A}$*.*

A QANIZK is a NIZK for a class of languages. The common reference string crs is allowed to depend on the language, but for the zero-knowledge property there has to be a single simulator for all the entire class.

More formally, let $\mathcal{D}_{\mathsf{par}}$ be a probability distribution on a class of languages $\{\mathcal{L}_\rho\}$ where ρ is a description of each language. The languages $\mathcal{L}_\rho$ are defined via a witness relation $\mathcal{R}_\rho$, i.e. $\mathcal{L}_\rho := \{x \mid \exists w : (x, w) \in \mathcal{R}_\rho\}$. For the case of linear subspaces we have $\mathcal{R}_{[\mathbf{A}]_1} = ([\mathbf{Ar}]_1, \mathbf{r}) \in \mathbb{G}_1^m \times \mathbb{Z}_q^n$ for a matrix $\mathbf{A}$ generated by a $\mathcal{D}_{m,n}$ matrix distribution. The languages are described by $[\mathbf{A}]_1$. The parameters par contain a description of $\mathbb{G}_1$.

Definition 15. *A* quasi-adaptive non-interactive zero-knowledge argument Π *for a language distribution* $\mathcal{D}_{\mathsf{par}}$ *is a five-tuple* $\Pi := (\mathsf{Gen}_{\mathsf{par}}, \mathsf{Gen}_{\mathsf{NIZK}}, \mathsf{Prove}, \mathsf{Ver}_{\mathsf{NIZK}}, \mathsf{Sim})$ *of polynomial time algorithms with the following properties:*

- *The probabilistic algorithm* $\mathsf{Gen}_{\mathsf{par}}(\lambda)$ *generates* par*.*
- *The probabilistic common reference string (crs) generator* $\mathsf{Gen}_{\mathsf{crs}}(\mathsf{par}, \rho)$ *generates a public crs* crs *and a secret trapdoor* td*. The crs implicitly defines a tag space* $\mathcal{T}$*.*
- *The probabilistic proof generating algorithm* $\mathsf{Prove}(\mathsf{crs}, \mathsf{tag} \in \mathcal{T}, (x, w) \in \mathcal{R}_\rho)$ *generates a proof* π *for the statement* $x \in \mathcal{L}_\rho$*.*
- *The deterministic proof checking algorithm* $\mathsf{Ver}_{\mathsf{NIZK}}(\mathsf{crs}, \mathsf{tag} \in \mathcal{T}, x, \pi)$ *returns a bit, where* 1 *indicates a valid proof for* $x \in \mathcal{L}_\rho$*.*

$\underline{\text{INIT:}}$	$\underline{\text{SIM}(\mathsf{crs}, \mathsf{tag} \in \mathcal{T}, x):}$
$\mathsf{par} \xleftarrow{\$} \mathsf{Gen}_{\mathsf{par}}(\lambda)$	$\pi \xleftarrow{\$} \mathsf{Sim}(\mathsf{crs}, \mathsf{tag}, x, \mathsf{td})$
$\rho \xleftarrow{\$} \mathcal{D}_{\mathsf{par}}$	$\mathcal{P} := \mathcal{P} \cup (\mathsf{tag}, x, \pi)$
$(\mathsf{crs}, \mathsf{td}) \xleftarrow{\$} \mathsf{Gen}_{\mathsf{crs}}(\mathsf{par}, \rho)$	**return** π
return crs	
	$\underline{\text{FINALIZE}_{\mathsf{NIZK}}(\mathsf{tag}^\star, x^\star, \pi^\star):}$
	return $\mathsf{Ver}_{\mathsf{NIZK}}(\mathsf{crs}, \mathsf{tag}^\star, x^\star, \pi^\star) \stackrel{?}{=} 1$ $\wedge\, x^\star \notin \mathcal{L}_\rho \wedge (\mathsf{tag}^\star, x^\star, \pi^\star) \notin \mathcal{P}$

Fig. 27. The game USS for defining unbounded simulation-soundness for QANIZKs.

– *The probabilistic proof simulating algorithm* $\mathsf{Sim}(\mathsf{crs}, \mathsf{tag} \in \mathcal{T}, x, \mathsf{td})$ *generates proofs, but – in contrast to* Prove *– without using the witness, but with the trapdoor instead.*

For our purposes we require the QANIZK to satisfy the following three properties:

Definition 16 (Perfect Completeness). *A QANIZK* Π *is* perfectly complete *iff for all* λ*, all* par *output by* $\mathsf{Gen}_{\mathsf{par}}(\lambda)$*, all* ρ*, all tags* $\mathsf{tag} \in \mathcal{T}$ *and all* $(x, w) \in \mathcal{R}_\rho$*, we have*

$$\Pr[\mathsf{Ver}_{\mathsf{NIZK}}(\mathsf{crs}, \mathsf{tag} \in \mathcal{T}, x, \pi) = 1 \mid (\mathsf{crs}, \mathsf{td}) \xleftarrow{\$} \mathsf{Gen}_{\mathsf{crs}}(\mathsf{par}, \rho), \\ \pi \xleftarrow{\$} \mathsf{Prove}(\mathsf{crs}, \mathsf{tag} \in \mathcal{T}, (x, w) \in \mathcal{R}_\rho)] = 1$$

Definition 17 (Perfect Zero-knowledge). *A QANIZK* Π *is* perfectly zero-knowledge *iff for all* λ*, all* par *output by* $\mathsf{Gen}_{\mathsf{par}}(\lambda)$*, all* ρ*, all* $(\mathsf{crs}, \mathsf{td})$ *output by* $\mathsf{Gen}_{\mathsf{crs}}(\mathsf{par}, \rho)$*, all tags* $\mathsf{tag} \in \mathcal{T}$ *and all* $(x, w) \in \mathcal{R}_\rho$*, the output distribution of*

$$\mathsf{Ver}_{\mathsf{NIZK}}(\mathsf{crs}, \mathsf{tag} \in \mathcal{T}, x, \pi) \text{ and } \mathsf{Sim}(\mathsf{crs}, \mathsf{tag} \in \mathcal{T}, x, \mathsf{td})$$

is identical.

Definition 18 (Unbounded Simulation-soundness). *A QANIZK* Π *is* unbounded simulation-soundness *(USS) iff for all PPT adversaries* $\mathcal{A}$*,*

$$\mathsf{Adv}^{\mathsf{uss}}_{\Pi}(\mathcal{A}) := \Pr\left[\mathsf{USS}^{\mathcal{A}} \Rightarrow 1\right]$$

is negligible. The game USS *is defined in Figure 27.*

The definition of USS is the stronger variant of [25], where the simulator oracle can be asked for proofs with the challenge tag $\mathsf{tag}^\star$ as well.

An efficient USS QANIZK for linear subspaces is Π_{uss}, shown in Figure 28. It was proposed by [14] and slightly modified by [25] to match the stronger USS definition. It makes use of a hash function $\mathcal{H} := (\mathsf{HGen}, \mathsf{HEval})$ with domain $\mathcal{T} \times \mathbb{G}_1^m \times \mathbb{G}_1^k$ and range $\{0,1\}^\gamma$.

$\underline{\mathsf{Gen}_{\mathsf{crs}}\big(\mathcal{PG}, [\mathbf{A}]_1 \in \mathbb{G}_1^{m\times n}\big)\colon}$
parse $\mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
$\mathcal{K} \xleftarrow{\$} \mathsf{HGen}\big(1^\lambda\big)$
$\mathbf{M}, \mathbf{N} \xleftarrow{\$} \mathcal{D}_k;\ \mathbf{K} \xleftarrow{\$} \mathbb{Z}_q^{m\times(k+1)}$
for $j \in \{1, \ldots, \gamma\}, b \in \{0,1\}$ **do**
$\big\lfloor \mathbf{K}_{j,b} \xleftarrow{\$} \mathbb{Z}_q^{k\times(k+1)}$
$\mathsf{crs} := \Big(\mathcal{K}, [\mathbf{M}]_2, [\mathbf{KM}]_2, \big[\overline{\mathbf{N}}\big]_1, \big[\mathbf{A}^\top\mathbf{K}\big]_1$
$\Big(\big[\mathbf{K}_{j,b}\mathbf{M}\big]_2, \big[\overline{\mathbf{N}}^\top\mathbf{K}_{j,b}\big]_1\Big)_{1\le j\le\gamma, b\in\{0,1\}}\Big)$
$\mathsf{td} := \mathbf{K}$
return $(\mathsf{crs}, \mathsf{td})$

$\underline{\mathsf{Prove}\big(\mathsf{crs}, \mathsf{tag} \in \mathcal{T}, [\mathbf{c}]_1 \in \mathbb{G}_1^m, \mathbf{r} \in \mathbb{Z}_q^n\big)\colon}$
assert $\mathbf{c} \stackrel{?}{=} \mathbf{Ar}$
$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k;\ \mathbf{t} := \overline{\mathbf{N}}\mathbf{s}$
$\tau := \mathsf{HEval}_{\mathcal{K}}\big(\mathsf{tag}, [\mathbf{c}]_1, [\mathbf{t}]_1\big)$
$\mathbf{u} := \mathbf{s}^\top \sum_{j=1}^{\gamma} \overline{\mathbf{N}}^\top \mathbf{K}_{j,\tau_j} + \mathbf{r}^\top \mathbf{A}^\top \mathbf{K}$
return $\pi := \big([\mathbf{t}]_1, [\mathbf{u}]_1\big)$

$\underline{\mathsf{Ver}_{\mathsf{NIZK}}\big(\mathsf{crs}, \mathsf{tag}, [\mathbf{c}]_1 \in \mathbb{G}_1^m, \mathbf{r} \in \mathbb{Z}_q^n, \pi\big)\colon}$
parse $\pi =: \big([\mathbf{t}]_1, [\mathbf{u}]_1\big)$
$\tau := \mathsf{HEval}_{\mathcal{K}}\big(\mathsf{tag}, [\mathbf{c}]_1, [\mathbf{t}]_1\big)$
return $e\big([\mathbf{u}]_1, [\mathbf{M}]_2\big) \stackrel{?}{=} e\big(\big[\mathbf{c}^\top\big]_1, [\mathbf{KM}]_2\big)$
$+ e\Big(\big[\mathbf{t}^\top\big]_1, \Big[\sum_{j=1}^{\gamma} \mathbf{K}_{j,\tau_j}\mathbf{M}\Big]_2\Big)$

$\underline{\mathsf{Sim}\big(\mathsf{crs}, \mathsf{td}, \mathsf{tag} \in \mathcal{T}, [\mathbf{c}]_1 \in \mathbb{G}_1^m\big)\colon}$
$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k;\ \mathbf{t} := \overline{\mathbf{N}}\mathbf{s}$
$\tau := \mathsf{HEval}_{\mathcal{K}}\big(\mathsf{tag}, [\mathbf{c}]_1, [\mathbf{t}]_1\big)$
$\mathbf{u} := \mathbf{s}^\top \sum_{j=1}^{\gamma} \overline{\mathbf{N}}^\top \mathbf{K}_{j,\tau_j} + \mathbf{c}^\top \mathbf{K}$
return $\pi := \big([\mathbf{t}]_1, [\mathbf{u}]_1\big)$

Fig. 28. The USS QANIZK Π_{uss}.

Theorem 8 ([14,25]). *The QANIZK Π_{uss} is perfectly complete, prefectly zero-knowledge and – if $\mathbf{A}$ was sampled with a $\mathcal{D}_{m,n}$ matrix distribution – unbounded simulation soundness under the $\mathcal{D}_k$-MDDH assumption for $\mathbb{G}_1$, the $\mathcal{D}_k$-MDDH assumption for $\mathbb{G}_2$ and the collision resistance of $\mathcal{H}$. More precisely, for all adversaries $\mathcal{A}$ there exist adversaries $\mathcal{B}_1$, $\mathcal{B}_2$ and $\mathcal{B}_3$ with*

$$\mathsf{Adv}^{\mathsf{uss}}_{\Pi_{\mathsf{uss}}}(\mathcal{A}) \leq \mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{D}_k,\mathsf{PGGen},2}(\mathcal{B}_1) + 4\gamma\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{D}_k,\mathsf{PGGen},1}(\mathcal{B}_2) + \mathsf{Adv}^{\mathsf{cr}}_{\mathcal{H}}(\mathcal{B}_3) + 2^{-\Omega(\lambda)}$$

and $T(\mathcal{B}_1) \approx T(\mathcal{B}_2) \approx T(\mathcal{B}_3) \approx T(\mathcal{A}) + Q_s \cdot \mathsf{poly}(\lambda)$, where Q_s denotes the number of Sim *queries of $\mathcal{A}$ and* poly *is a polynomial independent of $\mathcal{A}$.*

Any affine MAC with levels can be transformed with a USS QANIZK for linear subspaces $\Pi := (\mathsf{Gen}_{\mathsf{par}}, \mathsf{Gen}_{\mathsf{NIZK}}, \mathsf{Prove}, \mathsf{Ver}_{\mathsf{NIZK}}, \mathsf{Sim})$ tightly to an IND-HID-CCCA-secure hierarchical identity-based key encapsulation mechanism (HIBKEM) under the $\mathcal{D}_{k+\eta,k}$-MDDH assumption in $\mathbb{G}_1$. The transformation is shown in Figure 29. It is a straightforward generalization of the one in [25]. We only consider HIBKEM here, and one can prove that every IND-HID-CCCA-secure HIBKEM can be transformed (tightly) to an IND-HID-CCA-secure HIBE scheme with a (one-time secure) authenticated symmetric cipher by adapting a similar transformation for public-key encryption in [26].

Theorem 9 (Delegation Invariance). *For an affine MAC with levels* MAC*, the HIBKEM* $\mathsf{HIBKEM}_{\mathsf{CCA}}[\mathsf{MAC}, \mathcal{D}_{k+\eta,k}]$ *is delegation invariant.*

Proof. The proof is identical to Theorem 5, because the user secret keys are identical to $\mathsf{HIBKEM}_{\mathsf{CPA}}[\mathsf{MAC}, \mathcal{D}_{k+\eta,k}]$. □

Theorem 10 (Correctness). *The HIBKEM* $\mathsf{HIBKEM}_{\mathsf{CCA}}[\mathsf{MAC}, \mathcal{D}_{k+\eta,k}]$ *is correct.*

Proof. The Dec algorithm will never return $\perp$ for ciphertexts generated by Enc due to the perfect completeness of the QANIZK. The remaining argument is identical to Theorem 6. □

Theorem 11 (Security). *The HIBKEM* $\mathsf{HIBKEM}_{\mathsf{CCA}}[\mathsf{MAC}, \mathcal{D}_{k+\eta,k}]$ *is* IND-HID-CCCA *secure under the $\mathcal{D}_{k+\eta,k}$-MDDH assumption for $\mathbb{G}_1$ if* MAC *is* mHPR-CMA *secure and Π is zero-knowledge und unbounded simulation-sound. More precisely, for all adversaries $\mathcal{A}$ there exist adversaries $\mathcal{B}_1$, $\mathcal{B}_2$, and $\mathcal{B}_3$ with*

$$\mathsf{Adv}^{\mathsf{mind\text{-}hid\text{-}ccca}}_{\mathsf{HIBKEM}_{\mathsf{CPA}}[\mathsf{MAC},\mathcal{D}_{k+\eta,k}]}(\mathcal{A}) \leq \mathsf{Adv}^{\mathsf{mhpr\text{-}cma}}_{\mathsf{MAC},\mathsf{PGGen}}(\mathcal{B}_1) + 2\eta\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{D}_{k+\eta,k},\mathsf{PGGen},1}(\mathcal{B}_2) \\ 2\mathsf{Adv}^{\mathsf{uss}}_{\Pi}(\mathcal{B}_3) + 4Q_d\mathsf{uncert}(\mathcal{A}) + \frac{4}{q-1}$$

and $T(\mathcal{B}_1) \approx T(\mathcal{B}_2) \approx T(\mathcal{A}) + (Q_e + Q_c + Q_d) \cdot \mathsf{poly}(\lambda)$, where Q_e resp. Q_c resp. Q_d denotes the number of Eval *resp.* Chal *resp.* Dec *queries of $\mathcal{A}$ and* poly *is a polynomial independent of $\mathcal{A}$.*

$\underline{\mathsf{Gen}\big(1^\lambda\big)}$:
$(\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,q,P_1,P_2,e) := \mathcal{PG} \xleftarrow{\$} \mathsf{PGGen}\big(1^\lambda\big)$
$\mathsf{sk}_{\mathsf{MAC}} \xleftarrow{\$} \mathsf{Gen}_{\mathsf{MAC}}(\mathbb{G}_2,q,P_2)$
$\mathsf{sk}_{\mathsf{MAC}} =: \Big(\mathbf{B},(\mathbf{X}_{l,i,j})_{\substack{1\le l\le \ell(p),1\le i\le L,\\ 1\le j\le \ell'(l,i)}},\mathbf{x}'\Big)$
$\mathbf{A} \xleftarrow{\$} \mathcal{D}_{k+\eta,k}$; $(\mathsf{crs},\mathsf{td}) \xleftarrow{\$} \mathsf{Gen}_{\mathsf{crs}}(\mathcal{PG},\mathbf{A})$
for $l \in \{1,\dots,\ell(L)\},\ i \in \{1,\dots,L\},\ j \in \{1,\dots,\ell'(l,i)\}$ **do**
  $\mathbf{Y}_{l,i,j} \xleftarrow{\$} \mathbb{Z}_q^{k\times n}$; $\mathbf{Z}_{l,i,j} := \big(\mathbf{Y}_{l,i,j}^\top \mid \mathbf{X}_{l,i,j}^\top\big)\mathbf{A}$
  $\mathbf{D}_{l,i,j} := \mathbf{X}_{l,i,j}\cdot\mathbf{B}$; $\mathbf{E}_{l,i,j} := \mathbf{Y}_{l,i,j}\cdot\mathbf{B}$
$\mathbf{y}' \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{z}' := \big(\mathbf{y}'^\top \mid \mathbf{x}'^\top\big)\cdot\mathbf{A}$
$\widetilde{\mathbf{Z}} := \big([\mathbf{Z}_{l,i,j}]_1\big)_{1\le l\le\ell(p),1\le i\le L,1\le j\le\ell'(l,i)}$
$\mathsf{pk} := \Big(\mathsf{crs},\mathcal{PG},[\mathbf{A}]_1,\widetilde{\mathbf{Z}},[\mathbf{z}']_1\Big)$
$\widetilde{\mathsf{dk}} := \big([\mathbf{D}_{l,i,j}]_2,[\mathbf{E}_{l,i,j}]_2\big)_{\substack{1\le l\le\ell(p),1\le i\le L,\\ 1\le j\le\ell'(l,i)}}$
$\mathsf{dk} := \Big([\mathbf{B}]_2,\widetilde{\mathsf{dk}}\Big)$
$\mathsf{sk} := \Big(\mathsf{sk}_{\mathsf{MAC}},(\mathbf{Y}_{l,i,j})_{\substack{1\le l\le\ell(p),1\le i\le L,\\ 1\le j\le\ell'(l,i)}},\mathbf{y}'\Big)$
return $(\mathsf{pk},\mathsf{dk},\mathsf{sk})$

$\underline{\mathsf{Ext}(\mathsf{sk},\mathsf{id}\in\mathcal{S}^p)}$:
$\Big(\big([\mathbf{t}_l]_2\big)_{1\le l\le\ell(p)},[\mathbf{u}]_2\Big) \xleftarrow{\$} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}},\mathsf{id})$
$\mathbf{v} := \sum_{l=1}^{\ell(p)}\Big(\sum_{i=1}^{p}\sum_{j=1}^{\ell'(l,i)} f_{l,i,j}\big(\mathsf{id}_{|i}\big)\mathbf{Y}_{l,i,j}\Big)\mathbf{t}_l + \mathbf{y}'$
for $l \in \{1,\dots,\ell(p)\},\ i \in \{p+1,\dots,L\},\ j \in \{1,\dots,\ell'(l,i)\}$ **do**
  $\mathbf{d}_{l,i,j} := \mathbf{X}_{l,i,j}\mathbf{t}_l$; $\mathbf{e}_{l,i,j} := \mathbf{Y}_{l,i,j}\mathbf{t}_l$
$\mathsf{usk}[\mathsf{id}] := \Big(\big([\mathbf{t}_l]_2\big)_{1\le l\le\ell(p)},[\mathbf{u}]_2,[\mathbf{v}]_2\Big)$
$\mathsf{udk}[\mathsf{id}] := \big([\mathbf{d}_{l,i,j}]_2,[\mathbf{e}_{l,i,j}]_2\big)_{\substack{1\le l\le\ell(p),\\ p+1\le i\le L,\\ 1\le j\le\ell'(l,i)}}$
return $(\mathsf{usk}[\mathsf{id}],\mathsf{udk}[\mathsf{id}])$

$\underline{\mathsf{Enc}(\mathsf{pk},\mathsf{id}\in\mathcal{S}^p)}$:
$\mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{c}_0 := \mathbf{A}\mathbf{r}$; $\mathsf{K} := \mathbf{z}'\cdot\mathbf{r}$
for $l \in \{1,\dots,\ell(p)\}$ **do**
  $\mathbf{c}_{1,l} := \sum_{i=1}^{p}\sum_{j=1}^{\ell'(l,i)} f_{l,i,j}\big(\mathsf{id}_{|i}\big)\mathbf{Z}_{l,i,j}\mathbf{r}$
$\pi \xleftarrow{\$} \mathsf{Prove}\Big(\mathsf{crs},\big([\mathbf{c}_{1,l}]_1\big)_{1\le l\le\ell(p)},[\mathbf{c}_0]_1,\mathbf{r}\Big)$
$\mathsf{C} := \Big(\pi,[\mathbf{c}_0]_1,\big([\mathbf{c}_{1,l}]_1\big)_{1\le l\le\ell(p)}\Big)$
return $\big([\mathsf{K}]_T,\mathsf{C}\big)$

$\underline{\mathsf{Del}(\mathsf{dk},\mathsf{usk}[\mathsf{id}],\mathsf{udk}[\mathsf{id}],\mathsf{id}\in\mathcal{S}^p,\mathsf{id}_{p+1})}$:
$\mathsf{usk}[\mathsf{id}] =: \Big(\big([\mathbf{t}_l]_2\big)_{1\le l\le\ell(p)},[\mathbf{u}]_2,[\mathbf{v}]_2\Big)$
$\mathsf{udk}[\mathsf{id}] =: \big([\mathbf{d}_{l,i,j}]_2,[\mathbf{e}_{l,i,j}]_2\big)_{\substack{1\le l\le\ell(p),\\ p+1\le i\le L,\\ 1\le j\le\ell'(l,i)}}$
for $l \in \{\ell(p)+1,\dots,\ell(p+1)\}$ **do** $\mathbf{t}_l := \mathbf{0}$
for $l \in \{1,\dots,\ell(p+1)\}$ **do**
  $\mathbf{s}_l' \xleftarrow{\$} \mathbb{Z}_q^{n'}$; $\mathbf{t}_l' := \mathbf{t}_l + \mathbf{B}\mathbf{s}_l'$
$\mathsf{id}' := (\mathsf{id}_1,\dots,\mathsf{id}_p,\mathsf{id}_{p+1})$
$\mathbf{u}' := \mathbf{u} + \sum_{l=1}^{\ell(p)}\sum_{j=1}^{\ell'(l,p+1)} f_{l,p+1,j}(\mathsf{id}')\mathbf{d}_{l,p+1,j}$
  $+ \sum_{l=1}^{\ell(p+1)}\Big(\sum_{i=1}^{p+1}\sum_{j=1}^{\ell'(l,i)} f_{l,i,j}\big(\mathsf{id}'_{|i}\big)\mathbf{D}_{l,i,j}\Big)\mathbf{s}_l'$
$\mathbf{v}' := \mathbf{v} + \sum_{l=1}^{\ell(p)}\sum_{j=1}^{\ell'(l,p+1)} f_{l,p+1,j}(\mathsf{id}')\mathbf{e}_{l,p+1,j}$
  $+ \sum_{l=1}^{\ell(p+1)}\Big(\sum_{i=1}^{p+1}\sum_{j=1}^{\ell'(l,i)} f_{l,i,j}\big(\mathsf{id}'_{|i}\big)\mathbf{E}_{l,i,j}\Big)\mathbf{s}_l'$
for $l \in \{1,\dots,\ell(p)\},\ i \in \{p+2,\dots,L\},\ j \in \{1,\dots,\ell'(l,i)\}$ **do**
  $\mathbf{d}'_{l,i,j} := \mathbf{d}_{l,i,j} + \mathbf{D}_{l,i,j}\mathbf{s}_l'$
  $\mathbf{e}'_{l,i,j} := \mathbf{e}_{l,i,j} + \mathbf{E}_{l,i,j}\mathbf{s}_l'$
for $l \in \{\ell(p)+1,\dots,\ell(p+1)\},\ i \in \{p+2,\dots,L\},\ j \in \{1,\dots,\ell'(l,i)\}$ **do**
  $\mathbf{d}'_{l,i,j} := \mathbf{D}_{l,i,j}\mathbf{s}_l'$; $\mathbf{e}'_{l,i,j} := \mathbf{E}_{l,i,j}\mathbf{s}_l'$
$\mathsf{usk}' := \Big(\big([\mathbf{t}_l']_2\big)_{1\le l\le\ell(p+1)},[\mathbf{u}']_2,[\mathbf{v}']_2\Big)$
$\mathsf{udk}' := \big(\big[\mathbf{d}'_{l,i,j}\big]_2,\big[\mathbf{e}'_{l,i,j}\big]_2\big)_{\substack{1\le l\le\ell(p+1),\\ p+2\le i\le L,\\ 1\le j\le\ell'(l,i)}}$
return $(\mathsf{usk}',\mathsf{udk}')$

$\underline{\mathsf{Dec}(\mathsf{usk}[\mathsf{id}],\mathsf{id}\in\mathcal{S}^p,\mathsf{C})}$:
$\mathsf{usk}[\mathsf{id}] =: \Big(\big([\mathbf{t}_l]_2\big)_{1\le l\le\ell(p)},[\mathbf{u}]_2,[\mathbf{v}]_2\Big)$
$\mathsf{C} =: \Big(\pi,[\mathbf{c}_0]_1,\big([\mathbf{c}_{1,l}]_1\big)_{1\le l\le\ell(p)}\Big)$
if $\mathsf{Ver}_{\mathsf{NIZK}}\Big(\mathsf{crs},\big([\mathbf{c}_{1,l}]_1\big)_{1\le l\le\ell(p)},[\mathbf{c}_0]_1,\pi\Big) = 0$ **then return** $\perp$
$[\mathsf{K}]_T := e\Big(\big[\mathbf{c}_0^\top\big]_1,\begin{bmatrix}\mathbf{v}\\ \mathbf{u}\end{bmatrix}_2\Big) - \sum_{l=1}^{\ell(p)} e\big(\big[\mathbf{c}_{1,l}^\top\big]_1,[\mathbf{t}_l]_2\big)$
return $[\mathsf{K}]_T$

Fig. 29. The Transformation $\mathsf{HIBKEM}_{\mathsf{CCA}}$ of an affine MAC with levels to an HIBKEM. Differences to the $\mathsf{HIBKEM}_{\mathsf{CPA}}$ transformation are highlighted gray.

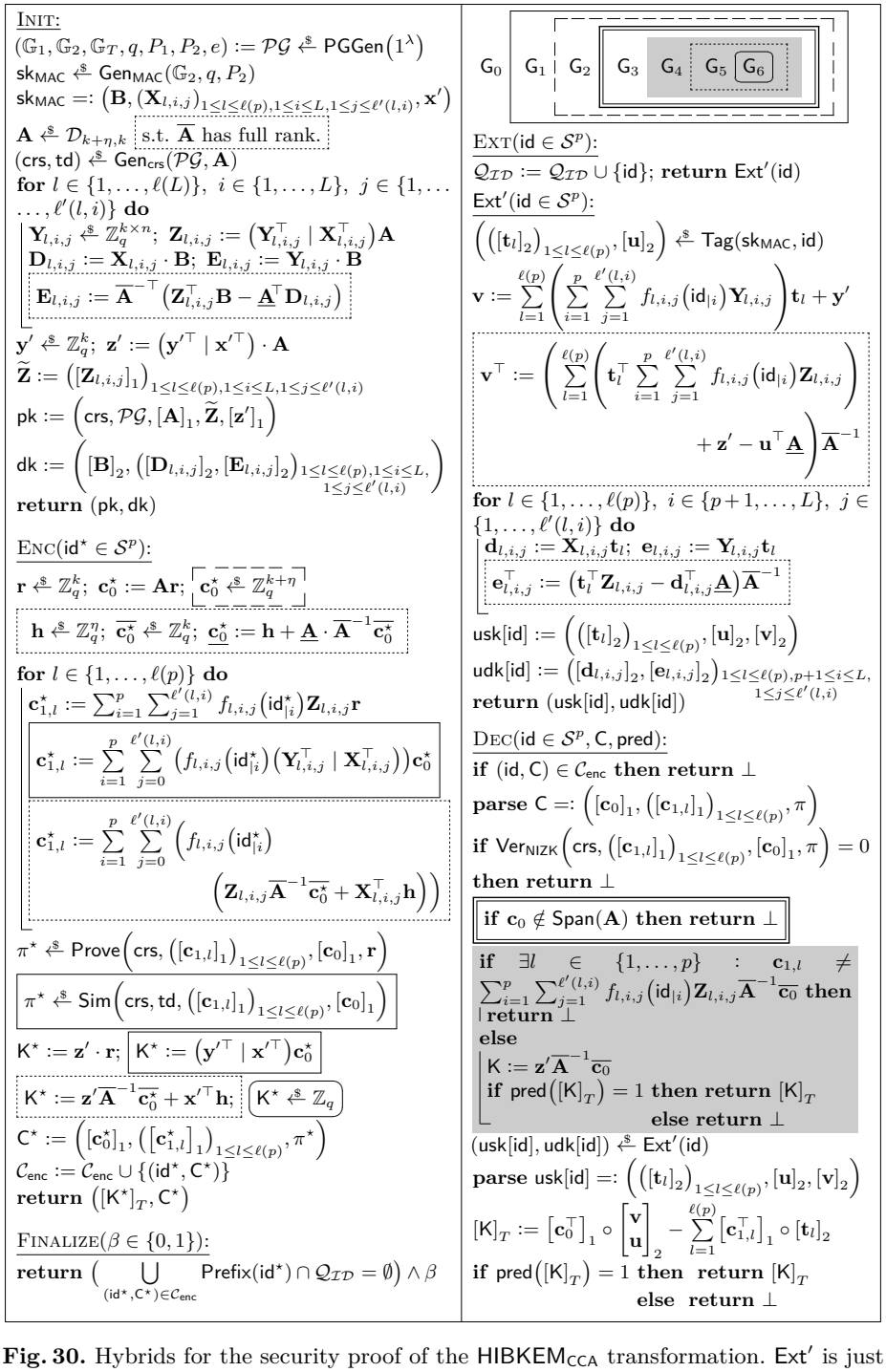


Fig. 30. Hybrids for the security proof of the $\mathsf{HIBKEM}_{\mathsf{CCA}}$ transformation. Ext' is just a helper function, not an oracle for the adversary.

Proof. The proof makes use of the hybrids G_0–G_6 defined in Figure 30. G_0 is the $\mathsf{IND\text{-}HID\text{-}CCCA}_{\mathsf{real}}$ game.

Lemma 64 ($\mathsf{G}_0 \rightsquigarrow \mathsf{G}_1$)**.**

$$\Pr\left[\mathsf{G}_0^{\mathcal{A}} \Rightarrow 1\right] = \Pr\left[\mathsf{G}_1^{\mathcal{A}} \Rightarrow 1\right]$$

Proof. The proof is identical to Lemma 60. □

Lemma 65 ($\mathsf{G}_1 \rightsquigarrow \mathsf{G}_2$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}_1^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_2^{\mathcal{A}} \Rightarrow 1\right]\right| \leq \eta \mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{D}_{k+\eta,k},\mathsf{PGGen},1}(\mathcal{B}) + \frac{1}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c + Q_d) \cdot \mathsf{poly}(\lambda)$.

Proof. In G_2 Sim is used to generate the QANIZK proofs in the Enc queries instead of Prove in G_1. The adversary can not notice the difference due to the perfect zero-knowledge of Π. The remaining argument is identical to Lemma 61. □

Lemma 66 ($\mathsf{G}_2 \rightsquigarrow \mathsf{G}_3$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}_2^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_3^{\mathcal{A}} \Rightarrow 1\right]\right| \leq \mathsf{Adv}^{\mathsf{uss}}_{\Pi}(\mathcal{B}) + Q_d \mathsf{uncert}(\mathcal{A})$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c + Q_d) \cdot \mathsf{poly}(\lambda)$.

Proof. A difference between G_2 and G_3 occurs iff the adversary issues a Dec query with $\left(\mathsf{id}, \mathsf{C} = \left(\pi, [\mathbf{c}_0]_1, \left([\mathbf{c}_{1,l}]_1\right)_{1 \leq l \leq \ell(p)}\right), \mathsf{pred}\right)$ where $(\mathsf{id}, \mathsf{C}) \notin \mathcal{C}_{\mathsf{enc}}$ and $\mathbf{c}_0 \notin \mathsf{Span}(\mathbf{A})$, but still $\mathsf{Ver}_{\mathsf{NIZK}}\left(\mathsf{crs}, \left([\mathbf{c}_{1,l}]_1\right)_{1 \leq l \leq \ell(p)}, [\mathbf{c}_0]_1, \pi\right) = 1$ and $\mathsf{pred}(\mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id}, \mathsf{C})) = 1$ for a valid user secret key $\mathsf{usk}[\mathsf{id}]$ for id. In this case, however, the adversary can be used to break the USS property of Π: The reduction can use the Sim oracle to compute the QANIZK proofs in the Enc queries. When the adversary issues the Dec query with $\left(\mathsf{id}, \mathsf{C} = \left(\pi, [\mathbf{c}_0]_1, \left([\mathbf{c}_{1,l}]_1\right)_{1 \leq l \leq \ell(p)}\right), \mathsf{pred}\right)$ that satisfies the above properties, we have to distinguish the following two cases:

– The ciphertext C was returned by the Enc oracle before for an identity $\mathsf{id}^\star \neq \mathsf{id}$. (If $\mathsf{id} = \mathsf{id}^\star$, the Dec query would not be allowed.) Let $\left([\mathbf{t}]_2, [\mathbf{u}]_2,\right.$

$[\mathbf{v}]_2\Big)$ be a user secret key for id. Then

$$\begin{aligned}
\mathsf{K} &= \mathbf{c}_0^\top \begin{pmatrix}\mathbf{v}\\ \mathbf{u}\end{pmatrix} - \sum_{l=1}^{\ell(p)} \mathbf{c}_{1,l}^\top \mathbf{t}_l \\
&= \mathbf{c}_0^\top \left(\sum_{l=1}^{\ell(p)} \sum_{i=1}^{p} \sum_{j=1}^{\ell'(l,i)} f_{l,i,j}\big(\mathsf{id}_{|i}\big) \begin{pmatrix}\mathbf{Y}_{l,i,j}\\ \mathbf{X}_{l,i,j}\end{pmatrix} \mathbf{t}_l + \begin{pmatrix}\mathbf{y}'\\ \mathbf{x}'\end{pmatrix} \right) \\
&\quad - \sum_{l=1}^{\ell(p)} \mathbf{c}_0^\top \sum_{i=1}^{p} \sum_{j=1}^{\ell'(l,i)} f_{l,i,j}\Big(\mathsf{id}^\star_{|i}\Big) \begin{pmatrix}\mathbf{Y}_{l,i,j}\\ \mathbf{X}_{l,i,j}\end{pmatrix} \mathbf{t}_l \\
&= \mathbf{c}_0^\top \begin{pmatrix}\mathbf{y}'\\ \mathbf{x}'\end{pmatrix} + \mathbf{c}_0^\top \sum_{l=1}^{\ell(p)} \sum_{i=1}^{p} \sum_{j=1}^{\ell'(l,i)} \left(f_{l,i,j}\big(\mathsf{id}_{|i}\big) - f_{l,i,j}\Big(\mathsf{id}^\star_{|i}\Big) \right) \begin{pmatrix}\mathbf{X}_{l,i,j}\\ \mathbf{Y}_{l,i,j}\end{pmatrix} \mathbf{t}_l \,.
\end{aligned}$$

Assume $\sum_{i=1}^{p} \sum_{j=1}^{\ell'(l,i)} \Big(f_{l,i,j}\big(\mathsf{id}_{|i}\big) - f_{l,i,j}\Big(\mathsf{id}^\star_{|i}\Big)\Big) \neq 0$ for a $l \in \{1,\dots,p\}$ – if such an l would not exist, the underlying affine MAC with levels could be trivially broken. Since $\mathbf{t}_l$ is a uniform random vector, K is uniformly random to the adversary. Thus DEC queries of this type are rejected due to $\mathsf{pred}([\mathsf{K}]_T) = 0$ anyway with probability at least $(1 - Q_d \mathsf{uncert}(\mathcal{A}))$. So in this case the adversary will not notice any difference between G_2 and G_3 for these queries.

– The ciphertext C was not returned by the ENC oracle before. In this case the ciphertext can be send to the $\textsc{Finalize}_{\mathsf{NIZK}}$ oracle to win the USS game.

□

Lemma 67 ($\mathsf{G}_3 \rightsquigarrow \mathsf{G}_4$)**.**

$$\big|\Pr\big[\mathsf{G}_3^{\mathcal{A}} \Rightarrow 1\big] - \Pr\big[\mathsf{G}_4^{\mathcal{A}} \Rightarrow 1\big]\big| \leq Q_d \mathsf{uncert}(\mathcal{A})$$

Proof. A difference between G_3 and G_4 occurs iff the adversary issues a DEC query with $\Big(\mathsf{id}, \mathsf{C} = \Big(\pi, [\mathbf{c}_0]_1, \big([\mathbf{c}_{1,l}]_1\big)_{1\leq l\leq \ell(p)}\Big), \mathsf{pred}\Big)$ where $(\mathsf{id}, \mathsf{C}) \notin \mathcal{C}_{\mathsf{enc}}$, $\mathbf{c}_0 \in \mathsf{Span}(\mathbf{A})$, and $\mathbf{c}_{1,l} \neq \sum_{i=1}^{p} \sum_{j=1}^{\ell'(l,i)} f_{l,i,j}\big(\mathsf{id}_{|i}\big) \mathbf{Z}_{l,i,j} \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}_0}$ for some $l \in \{1,\dots,p\}$, but still $\mathsf{Ver}_{\mathsf{NIZK}}\Big(\mathsf{crs}, \big([\mathbf{c}_{1,l}]_1\big)_{1\leq l\leq \ell(p)}, [\mathbf{c}_0]_1, \pi\Big) = 1$ and $\mathsf{pred}(\mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id}, \mathsf{C})) = 1$ for a valid user secret key $\mathsf{usk}[\mathsf{id}]$ for id. Let $\Big(\big([\mathbf{t}_l]_2\big)_{1\leq l\leq \ell(p)}, [\mathbf{u}]_2, [\mathbf{v}]_2\Big)$ be a user

secret key for id. Then

$$\begin{aligned}\mathsf{K} &= \mathbf{c}_0^\top \begin{pmatrix}\mathbf{v}\\ \mathbf{u}\end{pmatrix} - \sum_{l=1}^{\ell(p)} \mathbf{c}_{1,l}^\top \mathbf{t}_l \\ &= \mathbf{c}_0^\top \left(\sum_{l=1}^{\ell(p)} \sum_{i=1}^{p} \sum_{j=1}^{\ell'(l,i)} f_{l,i,j}\big(\mathsf{id}_{|i}\big) \begin{pmatrix}\mathbf{Y}_{l,i,j}\\ \mathbf{X}_{l,i,j}\end{pmatrix} \mathbf{t}_l + \begin{pmatrix}\mathbf{y}'\\ \mathbf{x}'\end{pmatrix} \right) - \sum_{l=1}^{\ell(p)} \mathbf{c}_{1,l}^\top \mathbf{t}_l \\ &\overset{(*)}{=} \mathbf{c}_0^\top \begin{pmatrix}\mathbf{y}'\\ \mathbf{x}'\end{pmatrix} + \sum_{l=1}^{\ell(p)} \underbrace{\left(\overline{\mathbf{c}_0}^\top \overline{\mathbf{A}}^{-\top} \sum_{i=1}^{p} \sum_{j=1}^{\ell'(l,i)} f_{l,i,j}\big(\mathsf{id}_{|i}\big) \mathbf{Z}_{l,i,j}^\top - \mathbf{c}_{1,l}^\top \right)}_{=:\Delta_l} \mathbf{t}_l \,.\end{aligned}$$

In step $(*)$ we use that $\mathbf{c}_0 \in \mathsf{Span}(\mathbf{A})$. A DEC query with the properties from above has $\Delta_l \neq \mathbf{0}$ for at least one l. Since $\mathbf{t}_l$ is uniformly random to the adversary, $\mathsf{pred}([\mathsf{K}]_T)$ can output 1 only with probability at most $Q_d \mathsf{uncert}(\mathcal{A})$.

In G_4 all DEC queries are answered without using a user secret key for the queried identity. □

Lemma 68 ($\mathsf{G}_4 \rightsquigarrow \mathsf{G}_5$)**.**

$$\big|\Pr\big[\mathsf{G}_4^{\mathcal{A}} \Rightarrow 1\big] - \Pr\big[\mathsf{G}_5^{\mathcal{A}} \Rightarrow 1\big]\big| \leq \frac{1}{q-1}$$

Proof. The proof is identical to Lemma 62. □

Lemma 69 ($\mathsf{G}_5 \rightsquigarrow \mathsf{G}_6$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\big|\Pr\big[\mathsf{G}_5^{\mathcal{A}} \Rightarrow 1\big] - \Pr\big[\mathsf{G}_6^{\mathcal{A}} \Rightarrow 1\big]\big| \leq \mathsf{Adv}^{\mathsf{mhpr\text{-}cma}}_{\mathsf{MAC},\mathsf{PGGen}}(\mathcal{B})$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c + Q_d) \cdot \mathsf{poly}(\lambda)$.

Proof. The proof is identical to Lemma 63. □

SUMMARY. To prove Theorem 11, we combine Lemmata 64–69 to change the challenge keys $\mathsf{K}^\star$ from real to random and then apply all Lemmata (except Lemma 69) in reverse order to get to the $\mathsf{IND\text{-}HID\text{-}CCCA}_{\mathsf{rand}}$ game. □

E Transformation to Anonymous HIBE

E.1 CPA-secure Transformation

Any $\mathsf{mAPR\text{-}CMA}$-secure delegatable affine MAC can be transformed tightly to an anonymous hierarchical identity-based key encapsulation mechanism (HIBKEM) under the $\mathcal{D}_{k+\eta,k}$-MDDH assumption in $\mathbb{G}_1$. The transformation is shown in Figure 31. It is identical to the one in [5], except that we consider multi-challenge security here.

$\underline{\mathsf{Gen}\left(1^\lambda\right)\text{:}}$
$\mathcal{PG} \xleftarrow{\$} \mathsf{PGGen}\left(1^\lambda\right)$
parse $\mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
$\mathsf{sk}_{\mathsf{MAC}} \xleftarrow{\$} \mathsf{Gen}_{\mathsf{MAC}}(\mathbb{G}_2, q, P_2)$
$\mathsf{sk}_{\mathsf{MAC}} =: \left(\mathbf{B}, (\mathbf{X}_{i,j})_{1\le i\le L, 1\le j\le \ell'(i)}, \mathbf{x}'\right)$
$\mathbf{A} \xleftarrow{\$} \mathcal{D}_{k+\eta,k}$
for $i \in \{1,\dots,L\},\ j \in \{1,\dots,\ell'(i)\}$ **do**
  $\mathbf{Y}_{i,j} \xleftarrow{\$} \mathbb{Z}_q^{k\times n};\ \mathbf{Z}_{i,j} := \left(\mathbf{Y}_{i,j}^\top \mid \mathbf{X}_{i,j}^\top\right)\mathbf{A}$
$\mathbf{y}' \xleftarrow{\$} \mathbb{Z}_q^k;\ \mathbf{z}' := \left(\mathbf{y}'^\top \mid \mathbf{x}'^\top\right)\cdot\mathbf{A}$
$\widetilde{\mathbf{Z}} := \left([\mathbf{Z}_{i,j}]_1\right)_{1\le i\le L, 1\le j\le \ell'(i)}$
$\mathsf{pk} := \left(\mathcal{PG}, [\mathbf{A}]_1, \widetilde{\mathbf{Z}}, [\mathbf{z}']_1\right)$
$\mathsf{sk} := \left(\mathsf{sk}_{\mathsf{MAC}}, (\mathbf{Y}_{i,j})_{1\le i\le L, 1\le j\le \ell'(i)}, \mathbf{y}'\right)$
return $(\mathsf{pk}, \mathsf{sk})$

$\underline{\mathsf{Ext}(\mathsf{sk}, \mathsf{id} \in \mathcal{S}^p)\text{:}}$
$\left([\mathbf{t}]_2, [\mathbf{u}]_2\right) \xleftarrow{\$} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{id})$
$\mathbf{S} \xleftarrow{\$} \mathsf{GL}_{n'}(\mathbb{Z}_q);\ \mathbf{T} := \mathbf{B}\cdot\mathbf{S}$
$\mathbf{U} := \sum_{i=1}^{p}\sum_{j=1}^{\ell'(i)} f_{i,j}\left(\mathsf{m}_{|i}\right)\mathbf{X}_{i,j}\mathbf{T}$
$\mathbf{v} := \sum_{i=1}^{p}\sum_{j=1}^{\ell'(i)} f_{i,j}\left(\mathsf{id}_{|i}\right)\mathbf{Y}_{i,j}\mathbf{t} + \mathbf{y}'$
$\mathbf{V} := \sum_{i=1}^{p}\sum_{j=1}^{\ell'(i)} f_{i,j}\left(\mathsf{id}_{|i}\right)\mathbf{Y}_{i,j}\mathbf{T}$
for $i \in \{p+1,\dots,L\},\ j \in \{1,\dots,\ell'(i)\}$ **do**
  $\mathbf{d}_{i,j} := \mathbf{X}_{i,j}\mathbf{t};\ \mathbf{D}_{i,j} := \mathbf{X}_{i,j}\mathbf{T}$
  $\mathbf{e}_{i,j} := \mathbf{Y}_{i,j}\mathbf{t};\ \mathbf{E}_{i,j} := \mathbf{Y}_{i,j}\mathbf{T}$
$\mathsf{usk}[\mathsf{id}] := \left([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$
$\mathsf{udk}_1[\mathsf{id}] := \left([\mathbf{T}]_2, [\mathbf{U}]_2, [\mathbf{V}]_2\right)$
$\mathsf{udk}_2[\mathsf{id}] := \left([\mathbf{d}_{i,j}]_2, [\mathbf{D}_{i,j}]_2, [\mathbf{e}_{i,j}]_2, [\mathbf{E}_{i,j}]_2\right)_{p+1\le i\le L, 1\le j\le \ell'(i)}$
return $(\mathsf{usk}[\mathsf{id}], (\mathsf{udk}_1[\mathsf{id}], \mathsf{udk}_2[\mathsf{id}]))$

$\underline{\mathsf{Enc}(\mathsf{pk}, \mathsf{id} \in \mathcal{S}^p)\text{:}}$
$\mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^k;\ \mathbf{c}_0 := \mathbf{A}\mathbf{r}$
$\mathbf{c}_1 := \sum_{i=1}^{p}\sum_{j=1}^{\ell'(i)} f_{i,j}\left(\mathsf{id}_{|i}\right)\mathbf{Z}_{i,j}\mathbf{r}$
$\mathsf{K} := \mathbf{z}'\cdot\mathbf{r}$
return $\left([\mathsf{K}]_T, \mathsf{C} := \left([\mathbf{c}_0]_1, [\mathbf{c}_1]_1\right)\right)$

$\underline{\mathsf{Del}(\mathsf{dk}, \mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}], \mathsf{id} \in \mathcal{S}^p, \mathsf{id}_{p+1})\text{:}}$
parse $\mathsf{usk}[\mathsf{id}] =: \left([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$
parse $\mathsf{udk}[\mathsf{id}] =: \left([\mathbf{T}]_2, [\mathbf{U}]_2, [\mathbf{V}]_2, \mathsf{udk}_2\right)$
parse $\mathsf{udk}_2 =: \left([\mathbf{d}_{i,j}]_2, [\mathbf{D}_{i,j}]_2, [\mathbf{e}_{i,j}]_2, [\mathbf{E}_{i,j}]_2\right)_{p+1\le i\le L, 1\le j\le \ell'(i)}$
$\mathsf{id}' := (\mathsf{id}_1, \dots, \mathsf{id}_p, \mathsf{id}_{p+1})$
$\mathbf{u}' := \mathbf{u} + \sum_{j=1}^{\ell'(p+1)} f_{p+1,j}(\mathsf{id}')\mathbf{d}_{p+1,j}$
$\mathbf{U}' := \mathbf{U} + \sum_{j=1}^{\ell'(p+1)} f_{p+1,j}(\mathsf{id}')\mathbf{D}_{p+1,j}$
$\mathbf{v}' := \mathbf{v} + \sum_{j=1}^{\ell'(p+1)} f_{p+1,j}(\mathsf{id}')\mathbf{e}_{p+1,j}$
$\mathbf{V}' := \mathbf{V} + \sum_{j=1}^{\ell'(p+1)} f_{p+1,j}(\mathsf{id}')\mathbf{E}_{p+1,j}$
$\mathbf{s}' \xleftarrow{\$} \mathbb{Z}_q^{n'};\ \mathbf{t}' := \mathbf{t} + \mathbf{T}\cdot\mathbf{s}'$
$\mathbf{S}' \xleftarrow{\$} \mathsf{GL}_{n'}(\mathbb{Z}_q);\ \mathbf{T}' := \mathbf{T}\mathbf{S}'$
$\mathbf{u}'' := \mathbf{u} + \mathbf{U}\mathbf{s}';\ \mathbf{v} := \mathbf{v} + \mathbf{V}\mathbf{s}'$
$\mathbf{U} := \mathbf{U}\cdot\mathbf{S}';\ \mathbf{V} := \mathbf{V}\cdot\mathbf{S}'$
for $i \in \{p+2,\dots,L\},\ j \in \{1,\dots,\ell'(i)\}$ **do**
  $\mathbf{d}'_{i,j} := \mathbf{d}_{i,j} + \mathbf{D}_{i,j}\mathbf{s}'$
  $\mathbf{e}'_{i,j} := \mathbf{e}_{i,j} + \mathbf{E}_{i,j}\mathbf{s}'$
  $\mathbf{D}'_{i,j} := \mathbf{D}\cdot\mathbf{S}';\ \mathbf{E}'_{i,j} := \mathbf{E}\cdot\mathbf{S}'$
$\mathsf{usk}[\mathsf{id}'] := \left([\mathbf{t}']_2, [\mathbf{u}'']_2, [\mathbf{v}'']_2\right)$
$\mathsf{udk}_1[\mathsf{id}'] := \left([\mathbf{T}']_2, [\mathbf{U}'']_2, [\mathbf{V}'']_2\right)$
$\mathsf{udk}_2[\mathsf{id}'] =: \left(\left[\mathbf{d}'_{i,j}\right]_2, \left[\mathbf{D}'_{i,j}\right]_2, \left[\mathbf{e}'_{i,j}\right]_2, \left[\mathbf{E}'_{i,j}\right]_2\right)_{p+1\le i\le L, 1\le j\le \ell'(i)}$
return $(\mathsf{usk}[\mathsf{id}'], \mathsf{udk}_1[\mathsf{id}'], \mathsf{udk}_2[\mathsf{id}'])$

$\underline{\mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id} \in \mathcal{S}^p, \mathsf{C})\text{:}}$
parse $\mathsf{usk}[\mathsf{id}] =: \left([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$
parse $\mathsf{C} =: \left([\mathbf{c}_0]_1, [\mathbf{c}_1]_1\right)$
$[\mathsf{K}]_T := e\left(\left[\mathbf{c}_0^\top\right]_1, \begin{bmatrix}\mathbf{v}\\ \mathbf{u}\end{bmatrix}_2\right) - e\left(\left[\mathbf{c}_1^\top\right]_1, [\mathbf{t}]_2\right)$
return $[\mathsf{K}]_T$

Fig. 31. The Transformation $\mathsf{AHIBKEM}_{\mathsf{CPA}}$ of delegatable affine MAC to an HIBKEM.

Theorem 12 (Delegation Invariance). *For a delegatable affine MAC* MAC*, the HIBKEM* $\mathsf{AHIBKEM}_{\mathsf{CPA}}[\mathsf{MAC}, \mathcal{D}_{k+\eta,k}]$ *is delegation invariant.*

Proof. The user secret keys outputted by the Del algorithm are valid user secret keys with randomness $\mathbf{t}'$ and $\mathbf{T}'$, where $\mathbf{t}' := \mathbf{t} + \mathbf{T} \cdot \mathbf{s}'$. This is fresh random vector from $\mathsf{Span}(\mathbf{B})$ since $\mathbf{s}'$ is a fresh uniform random vector and $\mathsf{Span}(\mathbf{T}) = \mathsf{Span}(\mathbf{B})$. Furthermore $\mathbf{T}' := \mathbf{T}\mathbf{S}'$ is a fresh random matrix with $\mathsf{Span}(\mathbf{T}') = \mathsf{Span}(\mathbf{B})$, because $\mathbf{S}'$ is a uniform random matrix with full rank. □

Theorem 13 (Correctness). *The HIBKEM* $\mathsf{AHIBKEM}_{\mathsf{CPA}}[\mathsf{MAC}, \mathcal{D}_{k+\eta,k}]$ *is correct.*

Proof. The proof is identical to Theorem 6. □

Theorem 14 (Security). *The HIBKEM* $\mathsf{AHIBKEM}_{\mathsf{CPA}}[\mathsf{MAC}, \mathcal{D}_{k+\eta,k}]$ *is* mPR-HID-CPA *secure under the* $\mathcal{D}_{k+\eta,k}$-MDDH *assumption for* $\mathbb{G}_1$ *if* MAC *is* mAPR-CMA *secure. More precisely, for all adversaries* $\mathcal{A}$ *there exist adversaries* $\mathcal{B}_1$ *and* $\mathcal{B}_2$ *with*

$$\mathsf{Adv}^{\mathsf{pr\text{-}hid\text{-}cpa}}_{\mathsf{AHIBKEM}_{\mathsf{CPA}}[\mathsf{MAC},\mathcal{D}_{k+\eta,k}]}(\mathcal{A}) \leq \mathsf{Adv}^{\mathsf{mapr\text{-}cma}}_{\mathsf{MAC}}(\mathcal{B}_1) + \eta \mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{D}_{k+\eta,k},\mathsf{PGGen},1}(\mathcal{B}_2) + \frac{3}{q-1}$$

and $T(\mathcal{B}_1) \approx T(\mathcal{B}_2) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$*, where* Q_e *resp.* Q_c *denotes the number of* Eval *resp.* Chal *queries of* $\mathcal{A}$ *and* poly *is a polynomial independent of* $\mathcal{A}$*.*

Proof. The proof makes use of the hybrids G_0–G_4 defined in Figure 32. G_0 is the $\mathsf{mIND\text{-}HID\text{-}CPA}_{\mathsf{real}}$ game.

Lemma 70 ($\mathsf{G}_0 \rightsquigarrow \mathsf{G}_1$)**.**

$$\Pr\left[\mathsf{G}_0^{\mathcal{A}} \Rightarrow 1\right] = \Pr\left[\mathsf{G}_1^{\mathcal{A}} \Rightarrow 1\right]$$

Proof. The only difference between these games is that $\mathbf{c}_1^\star$ and $\mathsf{K}^\star$ are computed with the public value $\mathbf{Z}_{i,j}$ in game G_0 and with the secret key $\mathbf{X}_{i,j}$ and $\mathbf{Y}_{i,j}$ in G_1. □

Lemma 71 ($\mathsf{G}_1 \rightsquigarrow \mathsf{G}_2$)**.** *For all adversaries* $\mathcal{A}$ *there exists an adversary* $\mathcal{B}$ *with*

$$\left|\Pr\left[\mathsf{G}_1^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_2^{\mathcal{A}} \Rightarrow 1\right]\right| \leq \eta \mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{D}_{k+\eta,k},\mathsf{PGGen},1}(\mathcal{B}) + \frac{1}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$*.*

Proof. The only difference between these games is that $\mathbf{c}_0^\star$ is chosen from $\mathsf{Span}(\mathbf{A})$ in G_1 and from $\mathbb{Z}_q^{k+\eta}$ in G_2. This leads to a straightforward reduction to the Q_c-fold $\mathcal{D}_{k+\eta,k}$-MDDH assumption, where Q_c denotes the number of challenge queries.

The running time of $\mathcal{B}$ is dominated by the running time of $\mathcal{A}$ plus some (polynomial) overhead that is independent of $T(\mathcal{A})$ for the group operations in each oracle query. □

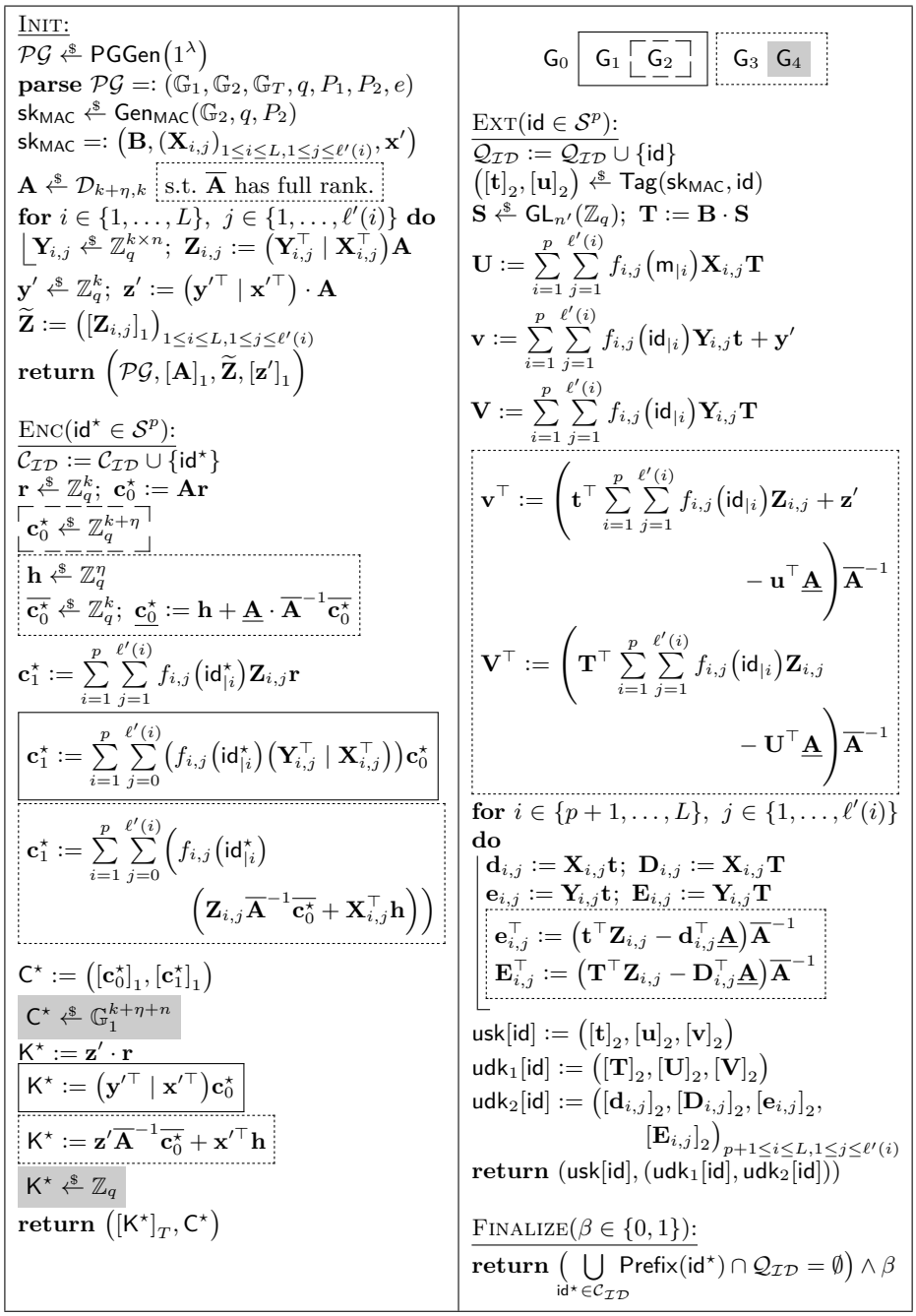


Fig. 32. Hybrids for the security proof of the $\mathsf{AHIBKEM}_{\mathsf{CPA}}$ transformation.

Lemma 72 ($\mathsf{G}_2 \rightsquigarrow \mathsf{G}_3$)**.**

$$\left|\Pr\left[\mathsf{G}_2^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_3^{\mathcal{A}} \Rightarrow 1\right]\right| \leq \frac{1}{q-1}$$

Proof. We assume from now on that $\overline{\mathbf{A}}$ has full rank. This happens with probability at least $(1 - 1/(q-1))$. Next notice that the values $\mathbf{Z}_{i,j}$ and $\mathbf{z}'$ are uniform random when $\mathbf{Y}_{i,j}$ and $\mathbf{y}'$ are hidden, so $\mathbf{Z}_{i,j}$ and $\mathbf{z}'$ are distributed identical in both games. Second notice

$$\mathbf{Z}_{i,j} := \left(\mathbf{Y}_{i,j}^\top \mid \mathbf{X}_{i,j}^\top\right) \cdot \mathbf{A} \iff \mathbf{Y}_{i,j}^\top = \left(\mathbf{Z}_{i,j} - \mathbf{X}_{i,j}^\top \underline{\mathbf{A}}\right)\overline{\mathbf{A}}^{-1}$$

and similarly

$$\mathbf{z}' := \left(\mathbf{y}'^\top \mid \mathbf{x}'^\top\right) \cdot \mathbf{A} \iff \mathbf{y}'^\top = \left(\mathbf{z}' - \mathbf{x}'^\top \underline{\mathbf{A}}\right)\overline{\mathbf{A}}^{-1}.$$

Game G_3 is obtained from G_2 by choosing $\mathbf{Z}_{i,j}$ and $\mathbf{z}'$ uniform random and replacing all occurrences of the values $\mathbf{Y}_{i,j}$ and $\mathbf{y}'$ by the terms described by the above equations. Thus the games are almost equally distributed. □

Lemma 73 ($\mathsf{G}_3 \rightsquigarrow \mathsf{G}_4$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}_3^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_4^{\mathcal{A}} \Rightarrow 1\right]\right| \leq \mathsf{Adv}^{\mathsf{mhpr\text{-}cma}}_{\mathsf{MAC},\mathsf{PGGen}}(\mathcal{B})$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c) \cdot \mathsf{poly}(\lambda)$.

Proof. The adversary $\mathcal{B}$ is given in Figure 33. When $\mathcal{B}$ plays the $\mathsf{mHPR\text{-}CMA}_{\mathsf{real}}$ game with the affine MAC with levels challenger, he simulates the game G_3 for $\mathcal{A}$. On the other hand, when $\mathcal{B}$ plays the $\mathsf{mHPR\text{-}CMA}_{\mathsf{rand}}$ game with the MAC challenger, he simulates the game G_4 for $\mathcal{A}$.

The running time of $\mathcal{B}$ is dominated by the running time of $\mathcal{A}$ plus some (polynomial) overhead that is independent of $T(\mathcal{A})$ for the group operations in each oracle query. □

Summary. To prove Theorem 14, we combine Lemmas 70–73 to change the challenge keys $\mathsf{K}^\star$ and ciphertexts $\mathsf{C}^\star$ from real to random and then apply all Lemmata (except Lemma 73) in reverse order to get to the $\mathsf{mPR\text{-}HID\text{-}CPA}_{\mathsf{rand}}$ game. Lemma 71 becomes an information theoretic argument then, because the values $\mathbf{c}_0^\star$ are hidden from the adversary when the challenge ciphertexts are chosen uniform random. □

E.2 CCA-secure Transformation

Like in the situation for non-anonymous HIBE, we can obtain an IND-HID-CCA-secure anonymous HIBE with the CHK-transformation using one-time signatures or with the [25] technique using USS QANIZKs.

Therefore we define the IND-AHID-CCCA-security for HIBE schemes. Unlike in the PR-HID-CPA-security, we can not guarantee that the ciphertexts are pseudorandom, because the proofs are not pseudorandom. However, we can still guarantee that the target identity is computationally hidden from the adversary, which is enough for anonymity.

$\underline{\text{INIT:}}$
$\mathcal{PG} \xleftarrow{\$} \text{INIT}_{\mathsf{MAC}}$
parse $\mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
$\mathbf{A} \xleftarrow{\$} \mathcal{D}_{k+\eta,k}$
for $i \in \{1, \dots, L\},\ j \in \{1, \dots, \ell'(i)\}$ **do**
$\left\lfloor \mathbf{Z}_{i,j} \xleftarrow{\$} \mathbb{Z}_q^{n \times k} \right.$
$\mathbf{z}' \xleftarrow{\$} \mathbb{Z}_q^{1 \times (k+\eta)}$
$\widetilde{\mathbf{Z}} := \left([\mathbf{Z}_{i,j}]_1\right)_{1 \le i \le L, 1 \le j \le \ell'(i)}$
return $\mathsf{pk} := \left(\mathcal{PG}, [\mathbf{A}]_1, \widetilde{\mathbf{Z}}, [\mathbf{z}']_1\right)$

$\underline{\text{ENC}(\mathsf{id}^\star \in \mathcal{S}^p):}$
$\mathbf{H} \xleftarrow{\$} \text{CHAL}(\mathsf{id}^\star)$
parse $\mathbf{H} =: \left([\mathbf{h}]_1, [\mathbf{h}_0]_1, [h_1]_T\right)$
$\overline{\mathbf{c}_0^\star} \xleftarrow{\$} \mathbb{Z}_q^k;\ \underline{\mathbf{c}_0^\star} := \mathbf{h} + \underline{\mathbf{A}} \cdot \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}_0^\star}$
$\mathbf{c}_1^\star := \left(\sum_{i=1}^{p} \sum_{j=0}^{\ell'(i)} f_{i,j}\left(\mathsf{id}_{|i}^\star\right) \mathbf{Z}_{i,j} \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}_0^\star}\right) + \mathbf{h}_0$
$\mathsf{K}^\star := \mathbf{z}' \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}_0^\star} + h_1$
return $\left([\mathsf{K}^\star]_T, \left([\mathbf{c}_0^\star]_1, \left([\mathbf{c}_1^\star]_1\right)_{1 \le \le \ell(p)}\right)\right)$

$\underline{\text{FINALIZE}(\beta \in \{0,1\}):}$
return $\text{FINALIZE}_{\mathsf{MAC}}(\beta)$

$\underline{\text{EXT}(\mathsf{id} \in \mathcal{S}^p):}$
$\left([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{T}]_2, [\mathbf{U}]_2, \mathsf{tdk}\right) \xleftarrow{\$} \text{EVAL}(\mathsf{id})$
parse $\mathsf{tdk} =: \left([\mathbf{d}_{i,j}]_2, [\mathbf{D}_{i,j}]_2\right)_{\substack{p+1 \le i, \le L \\ 1 \le j \le \ell'(i)}}$
$\mathbf{v}^\top := \left(\sum_{=1}^{\ell(p)} \left(\mathbf{t}^\top \sum_{i=1}^{p} \sum_{j=1}^{\ell'(i)} f_{i,j}\left(\mathsf{id}_{|i}\right) \mathbf{Z}_{i,j}\right) + \mathbf{z}' - \mathbf{u}^\top \underline{\mathbf{A}}\right) \overline{\mathbf{A}}^{-1}$
$\mathbf{V}^\top := \left(\mathbf{T}^\top \sum_{i=1}^{p} \sum_{j=1}^{\ell'(i)} f_{i,j}\left(\mathsf{id}_{|i}\right) \mathbf{Z}_{i,j} - \mathbf{U}^\top \underline{\mathbf{A}}\right) \overline{\mathbf{A}}^{-1}$
for $i \in \{p{+}1, \dots, L\},\ j \in \{1, \dots, \ell'(i)\}$ **do**
$\left\lfloor \mathbf{e}_{i,j}^\top := \left(\mathbf{t}^\top \mathbf{Z}_{i,j} - \mathbf{d}_{i,j}^\top \underline{\mathbf{A}}\right) \overline{\mathbf{A}}^{-1} \right.$
$\left\lfloor \mathbf{E}_{i,j}^\top := \left(\mathbf{T}^\top \mathbf{Z}_{i,j} - \mathbf{D}_{i,j}^\top \underline{\mathbf{A}}\right) \overline{\mathbf{A}}^{-1} \right.$
$\mathsf{usk}[\mathsf{id}] := \left([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$
$\mathsf{udk}_1[\mathsf{id}] := \left([\mathbf{T}]_2, [\mathbf{U}]_2, [\mathbf{V}]_2\right)$
$\mathsf{udk}_2[\mathsf{id}] := \left([\mathbf{d}_{i,j}]_2, [\mathbf{D}_{i,j}]_2, [\mathbf{e}_{i,j}]_2, [\mathbf{E}_{i,j}]_2\right)_{p+1 \le i \le L, 1 \le j \le \ell'(i)}$
return $(\mathsf{usk}[\mathsf{id}], (\mathsf{udk}_1[\mathsf{id}], \mathsf{udk}_2[\mathsf{id}]))$

Fig. 33. Adversary $\mathcal{B}$ for Lemma 73.

INIT:
$(\mathsf{pk}, \mathsf{dk}, \mathsf{sk}) \xleftarrow{\$} \mathsf{Gen}(\lambda)$
return $(\mathsf{pk}, \mathsf{dk})$
 	
EXT(id):
$\mathcal{Q}_{\mathcal{ID}} \leftarrow \mathcal{Q}_{\mathcal{ID}} \cup \{\mathsf{id}\}$
return $(\mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}]) \xleftarrow{\$} \mathsf{Ext}(\mathsf{sk}, \mathsf{id})$
 	
ENC($\mathsf{id}_0^\star, \mathsf{id}_1^\star$):
$(\mathsf{K}^\star, \mathsf{C}^\star) \xleftarrow{\$} \mathsf{Enc}(\mathsf{pk}, \mathsf{id}_d^\star)$
$\mathcal{C}_{\mathsf{enc}} := \mathcal{C}_{\mathsf{enc}} \cup \{(\mathsf{id}_0^\star, \mathsf{C}^\star), (\mathsf{id}_1^\star, \mathsf{C}^\star)\}$
if $d = 1$ **then** $\mathsf{K}^\star \xleftarrow{\$} \mathcal{K}$
return $(\mathsf{K}^\star, \mathsf{C}^\star)$
	DEC($\mathsf{id} \in \mathcal{S}^p, \mathsf{C}, \mathsf{pred}$):
	$(\mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}]) \xleftarrow{\$} \mathsf{Ext}(\mathsf{sk}, \mathsf{id})$
	$\mathsf{K} \xleftarrow{\$} \mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id}, \mathsf{C})$
	if $(\mathsf{id}, \mathsf{C}) \notin \mathcal{C}_{\mathsf{enc}} \wedge \mathsf{pred}(\mathsf{K}) = 1$ **then**
	$\quad$ **return** K
	else
	$\quad$ **return** $\perp$
	
	FINALIZE($\beta \in \{0,1\}$):
	return $\Big(\bigcup_{(\mathsf{id}^\star, \mathsf{C}^\star) \in \mathcal{C}_{\mathsf{enc}}} \mathsf{Prefix}(\mathsf{id}^\star) \cap \mathcal{Q}_{\mathcal{ID}} = \emptyset\Big) \wedge \beta$

Fig. 34. Games $\mathsf{mIND\text{-}AHID\text{-}CCCA}_d$ ($d \in \{0,1\}$) for defining mIND-AHID-CCCA security. In DEC the time need for evaluating the polynomial-time algorithm pred is charged to the adversaries run time.

Definition 19 (mIND-AHID-CCCA security). *An HIBKEM* HIBKEM *is* mIND-AHID-CCCA-secure *in* $\mathbb{G}_2$ *if for all PPT adversaries* $\mathcal{A}$ *where*

$$\mathsf{uncert}(\mathcal{A}) := \frac{1}{Q_d} \sum_{i=1}^{Q_d} \Pr_{\mathsf{K} \in \mathcal{K}}[\mathsf{pred}_i(\mathsf{K}) = 1]$$

is negligible in λ*, the function*

$$\mathsf{Adv}^{\mathsf{mind\text{-}hid\text{-}ccca}}_{\mathsf{HIBKEM}}(\mathcal{A}) := \Big| \Pr\Big[\mathsf{mIND\text{-}AHID\text{-}CCCA}_0^{\mathcal{A}} \Rightarrow 1\Big] - \Pr\Big[\mathsf{mIND\text{-}AHID\text{-}CCCA}_1^{\mathcal{A}} \Rightarrow 1\Big]\Big|$$

is negligible as well. The games $\mathsf{mIND\text{-}AHID\text{-}CCCA}_d$ *($d \in \{0,1\}$) are defined in Figure 34. The number of* DEC *queries of* $\mathcal{A}$ *is denoted by* Q_d *and* pred_i *($1 \le i \le Q_d$) is the* pred *algorithm of the* i*-th* DEC *query of* $\mathcal{A}$*.*

Any mAPR-CMA-secure delegatable affine MAC can be transformed with a USS QANIZK for linear subspaces $\Pi := (\mathsf{Gen}_{\mathsf{par}}, \mathsf{Gen}_{\mathsf{NIZK}}, \mathsf{Prove}, \mathsf{Ver}_{\mathsf{NIZK}}, \mathsf{Sim})$ tightly to an IND-AHID-CCCA-secure anonymous hierarchical identity-based key encapsulation mechanism (HIBKEM) under the $\mathcal{D}_{k+\eta,k}$-MDDH assumption in $\mathbb{G}_1$. The transformation is shown in Figure 35. It is a straightforward generalization of the one in [25].

Theorem 15 (Delegation Invariance). *For a delegatable affine MAC* MAC*, the HIBKEM* $\mathsf{AHIBKEM}_{\mathsf{CCA}}[\mathsf{MAC}, \mathcal{D}_{k+\eta,k}]$ *is delegation invariant.*

Proof. The proof is identical to Theorem 12, because the user secret keys are identical to $\mathsf{AHIBKEM}_{\mathsf{CCA}}[\mathsf{MAC}, \mathcal{D}_{k+\eta,k}]$. □

$\underline{\mathsf{Gen}\big(1^\lambda\big)\text{:}}$
$\mathcal{PG} \xleftarrow{\$} \mathsf{PGGen}\big(1^\lambda\big)$
parse $\mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
$\mathsf{sk}_{\mathsf{MAC}} \xleftarrow{\$} \mathsf{Gen}_{\mathsf{MAC}}(\mathbb{G}_2, q, P_2)$
$\mathsf{sk}_{\mathsf{MAC}} =: \big(\mathbf{B}, (\mathbf{X}_{i,j})_{1\le i\le L, 1\le j\le \ell'(i)}, \mathbf{x}'\big)$
$\mathbf{A} \xleftarrow{\$} \mathcal{D}_{k+\eta,k}$
$(\mathsf{crs}, \mathsf{td}) \xleftarrow{\$} \mathsf{Gen}_{\mathsf{crs}}(\mathcal{PG}, \mathbf{A})$
for $i \in \{1, \dots, L\},\ j \in \{1, \dots, \ell'(i)\}$ **do**
  $\mathbf{Y}_{i,j} \xleftarrow{\$} \mathbb{Z}_q^{k\times n};\ \mathbf{Z}_{i,j} := \big(\mathbf{Y}_{i,j}^\top \mid \mathbf{X}_{i,j}^\top\big)\mathbf{A}$
$\mathbf{y}' \xleftarrow{\$} \mathbb{Z}_q^k;\ \mathbf{z}' := \big(\mathbf{y}'^\top \mid \mathbf{x}'^\top\big) \cdot \mathbf{A}$
$\widetilde{\mathbf{Z}} := \big([\mathbf{Z}_{i,j}]_1\big)_{1\le i\le L, 1\le j\le \ell'(i)}$
$\mathsf{pk} := \Big(\mathsf{crs}, \mathcal{PG}, [\mathbf{A}]_1, \widetilde{\mathbf{Z}}, [\mathbf{z}']_1\Big)$
$\mathsf{sk} := \Big(\mathsf{sk}_{\mathsf{MAC}}, (\mathbf{Y}_{i,j})_{1\le i\le L, 1\le j\le \ell'(i)}, \mathbf{y}'\Big)$
return $(\mathsf{pk}, \mathsf{sk})$

$\underline{\mathsf{Ext}(\mathsf{sk}, \mathsf{id} \in \mathcal{S}^p)\text{:}}$
$\big([\mathbf{t}]_2, [\mathbf{u}]_2\big) \xleftarrow{\$} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{id})$
$\mathbf{S} \xleftarrow{\$} \mathsf{GL}_{n'}(\mathbb{Z}_q);\ \mathbf{T} := \mathbf{B} \cdot \mathbf{S}$
$\mathbf{U} := \sum_{i=1}^{p} \sum_{j=1}^{\ell'(i)} f_{i,j}\big(\mathsf{m}_{|i}\big)\mathbf{X}_{i,j}\mathbf{T}$
$\mathbf{v} := \sum_{i=1}^{p} \sum_{j=1}^{\ell'(i)} f_{i,j}\big(\mathsf{id}_{|i}\big)\mathbf{Y}_{i,j}\mathbf{t} + \mathbf{y}'$
$\mathbf{V} := \sum_{i=1}^{p} \sum_{j=1}^{\ell'(i)} f_{i,j}\big(\mathsf{id}_{|i}\big)\mathbf{Y}_{i,j}\mathbf{T}$
for $i \in \{p+1, \dots, L\},\ j \in \{1, \dots, \ell'(i)\}$ **do**
  $\mathbf{d}_{i,j} := \mathbf{X}_{i,j}\mathbf{t};\ \mathbf{D}_{i,j} := \mathbf{X}_{i,j}\mathbf{T}$
  $\mathbf{e}_{i,j} := \mathbf{Y}_{i,j}\mathbf{t};\ \mathbf{E}_{i,j} := \mathbf{Y}_{i,j}\mathbf{T}$
$\mathsf{usk}[\mathsf{id}] := \big([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{v}]_2\big)$
$\mathsf{udk}_1[\mathsf{id}] := \big([\mathbf{T}]_2, [\mathbf{U}]_2, [\mathbf{V}]_2\big)$
$\mathsf{udk}_2[\mathsf{id}] := \big([\mathbf{d}_{i,j}]_2, [\mathbf{D}_{i,j}]_2, [\mathbf{e}_{i,j}]_2, [\mathbf{E}_{i,j}]_2\big)_{p+1\le i\le L, 1\le j\le \ell'(i)}$
return $(\mathsf{usk}[\mathsf{id}], (\mathsf{udk}_1[\mathsf{id}], \mathsf{udk}_2[\mathsf{id}]))$

$\underline{\mathsf{Enc}(\mathsf{pk}, \mathsf{id} \in \mathcal{S}^p)\text{:}}$
$\mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^k;\ \mathbf{c}_0 := \mathbf{A}\mathbf{r}$
$\mathbf{c}_1 := \sum_{i=1}^{p} \sum_{j=1}^{\ell'(i)} f_{i,j}\big(\mathsf{id}_{|i}\big)\mathbf{Z}_{i,j}\mathbf{r}$
$\pi \xleftarrow{\$} \mathsf{Prove}\big(\mathsf{crs}, [\mathbf{c}_1]_1, [\mathbf{c}_0]_1, \mathbf{r}\big)$
$\mathsf{K} := \mathbf{z}' \cdot \mathbf{r}$
return $\big([\mathsf{K}]_T, \mathsf{C} := \big(\pi, [\mathbf{c}_0]_1, [\mathbf{c}_1]_1\big)\big)$

$\underline{\mathsf{Del}(\mathsf{dk}, \mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}], \mathsf{id} \in \mathcal{S}^p, \mathsf{id}_{p+1})\text{:}}$
parse $\mathsf{usk}[\mathsf{id}] =: \big([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{v}]_2\big)$
parse $\mathsf{udk}[\mathsf{id}] =: \big([\mathbf{T}]_2, [\mathbf{U}]_2, [\mathbf{V}]_2, \mathsf{udk}_2\big)$
parse $\mathsf{udk}_2 =: \big([\mathbf{d}_{i,j}]_2, [\mathbf{D}_{i,j}]_2, [\mathbf{e}_{i,j}]_2, [\mathbf{E}_{i,j}]_2\big)_{p+1\le i\le L, 1\le j\le \ell'(i)}$
$\mathsf{id}' := (\mathsf{id}_1, \dots, \mathsf{id}_p, \mathsf{id}_{p+1})$
$\mathbf{u}' := \mathbf{u} + \sum_{j=1}^{\ell'(p+1)} f_{p+1,j}(\mathsf{id}')\mathbf{d}_{p+1,j}$
$\mathbf{U}' := \mathbf{U} + \sum_{j=1}^{\ell'(p+1)} f_{p+1,j}(\mathsf{id}')\mathbf{D}_{p+1,j}$
$\mathbf{v}' := \mathbf{v} + \sum_{j=1}^{\ell'(p+1)} f_{p+1,j}(\mathsf{id}')\mathbf{e}_{p+1,j}$
$\mathbf{V}' := \mathbf{V} + \sum_{j=1}^{\ell'(p+1)} f_{p+1,j}(\mathsf{id}')\mathbf{E}_{p+1,j}$
$\mathbf{s}' \xleftarrow{\$} \mathbb{Z}_q^{n'};\ \mathbf{t}' := \mathbf{t} + \mathbf{T} \cdot \mathbf{s}'$
$\mathbf{S}' \xleftarrow{\$} \mathsf{GL}_{n'}(\mathbb{Z}_q);\ \mathbf{T}' := \mathbf{T}\mathbf{S}'$
$\mathbf{u}'' := \mathbf{u} + \mathbf{U}\mathbf{s}';\ \mathbf{v} := \mathbf{v} + \mathbf{V}\mathbf{s}'$
$\mathbf{U} := \mathbf{U} \cdot \mathbf{S}';\ \mathbf{V} := \mathbf{V} \cdot \mathbf{S}'$
for $i \in \{p+2, \dots, L\},\ j \in \{1, \dots, \ell'(i)\}$ **do**
  $\mathbf{d}'_{i,j} := \mathbf{d}_{i,j} + \mathbf{D}_{i,j}\mathbf{s}'$
  $\mathbf{e}'_{i,j} := \mathbf{e}_{i,j} + \mathbf{E}_{i,j}\mathbf{s}'$
  $\mathbf{D}'_{i,j} := \mathbf{D} \cdot \mathbf{S}';\ \mathbf{E}'_{i,j} := \mathbf{E} \cdot \mathbf{S}'$
$\mathsf{usk}[\mathsf{id}'] := \big([\mathbf{t}']_2, [\mathbf{u}'']_2, [\mathbf{v}'']_2\big)$
$\mathsf{udk}_1[\mathsf{id}'] := \big([\mathbf{T}']_2, [\mathbf{U}'']_2, [\mathbf{V}'']_2\big)$
$\mathsf{udk}_2[\mathsf{id}'] =: \big(\big[\mathbf{d}'_{i,j}\big]_2, \big[\mathbf{D}'_{i,j}\big]_2, \big[\mathbf{e}'_{i,j}\big]_2, \big[\mathbf{E}'_{i,j}\big]_2\big)_{p+1\le i\le L, 1\le j\le \ell'(i)}$
return $(\mathsf{usk}[\mathsf{id}'], \mathsf{udk}_1[\mathsf{id}'], \mathsf{udk}_2[\mathsf{id}'])$

$\underline{\mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id} \in \mathcal{S}^p, \mathsf{C})\text{:}}$
parse $\mathsf{usk}[\mathsf{id}] =: \big([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{v}]_2\big)$
parse $\mathsf{C} =: \big(\pi, [\mathbf{c}_0]_1, [\mathbf{c}_1]_1\big)$
if $\mathsf{Ver}_{\mathsf{NIZK}}\big(\mathsf{crs}, [\mathbf{c}_1]_1, [\mathbf{c}_0]_1, \pi\big) = 0$ **then return** $\perp$
$[\mathsf{K}]_T := e\Big(\big[\mathbf{c}_0^\top\big]_1, \begin{bmatrix}\mathbf{v}\\ \mathbf{u}\end{bmatrix}_2\Big) - e\big(\big[\mathbf{c}_1^\top\big]_1, [\mathbf{t}]_2\big)$
return $[\mathsf{K}]_T$

Fig. 35. The Transformation $\mathsf{AHIBKEM}_{\mathsf{CCA}}$ of delegatable affine MAC to an HIBKEM. Differences to the $\mathsf{AHIBKEM}_{\mathsf{CPA}}$ transformation are highlighted gray.

Theorem 16 (Correctness). *The HIBKEM* $\mathsf{AHIBKEM}_{\mathsf{CCA}}[\mathsf{MAC}, \mathcal{D}_{k+\eta,k}]$ *is correct.*

Proof. The proof is identical to Theorem 10. □

Theorem 17 (Security). *The HIBKEM* $\mathsf{AHIBKEM}_{\mathsf{CCA}}[\mathsf{MAC}, \mathcal{D}_{k+\eta,k}]$ *is* mIND-AHID-CCCA *secure under the* $\mathcal{D}_{k+\eta,k}$-MDDH *assumption for* $\mathbb{G}_1$ *if* MAC *is* mAPR-CMA *secure and* Π *is zero-knowledge und unbounded simulation-sound. More precisely, for all adversaries* $\mathcal{A}$ *there exist adversaries* $\mathcal{B}_1$, $\mathcal{B}_2$, *and* $\mathcal{B}_3$ *with*

$$\mathsf{Adv}^{\mathsf{mind\text{-}ahid\text{-}ccca}}_{\mathsf{AHIBKEM}_{\mathsf{CCA}}[\mathsf{MAC},\mathcal{D}_{k+\eta,k}]}(\mathcal{A}) \leq \mathsf{Adv}^{\mathsf{mapr\text{-}cma}}_{\mathsf{MAC}}(\mathcal{B}_1) + 2\eta\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{D}_{k+\eta,k},\mathsf{PGGen},1}(\mathcal{B}_2) + 2\mathsf{Adv}^{\mathsf{uss}}_{\Pi}(\mathcal{B}_3) + 4Q_d\mathsf{uncert}(\mathcal{A}) + \frac{3}{q-1}$$

and $T(\mathcal{B}_1) \approx T(\mathcal{B}_2) \approx T(\mathcal{A}) + (Q_e + Q_c + Q_d) \cdot \mathsf{poly}(\lambda)$, *where* Q_e *resp.* Q_c *resp.* Q_d *denotes the number of* Eval *resp.* Chal *resp.* Dec *queries of* $\mathcal{A}$ *and* poly *is a polynomial independent of* $\mathcal{A}$.

Proof. The proof makes use of the hybrids G_0–G_6 defined in Figure 36. G_0 is the $\mathsf{mIND\text{-}AHID\text{-}CCCA}_0$ game.

Lemma 74 ($\mathsf{G}_0 \rightsquigarrow \mathsf{G}_1$)**.**

$$\Pr\left[\mathsf{G}_0^{\mathcal{A}} \Rightarrow 1\right] = \Pr\left[\mathsf{G}_1^{\mathcal{A}} \Rightarrow 1\right]$$

Proof. The proof is identical to Lemma 70. □

Lemma 75 ($\mathsf{G}_1 \rightsquigarrow \mathsf{G}_2$)**.** *For all adversaries* $\mathcal{A}$ *there exists an adversary* $\mathcal{B}$ *with*

$$\left|\Pr\left[\mathsf{G}_1^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_2^{\mathcal{A}} \Rightarrow 1\right]\right| \leq \eta\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{D}_{k+\eta,k},\mathsf{PGGen},1}(\mathcal{B}) + \frac{1}{q-1}$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c + Q_d) \cdot \mathsf{poly}(\lambda)$.

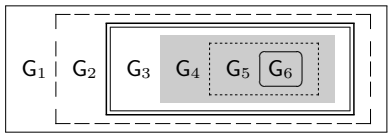
Proof. In G_2 Sim is used to generate the QANIZK proofs in the Enc queries instead of Prove in G_1. The adversary can not notice the difference due to the perfect zero-knowledge of Π. The remaining argument is identical to Lemma 71. □

Lemma 76 ($\mathsf{G}_2 \rightsquigarrow \mathsf{G}_3$)**.** *For all adversaries* $\mathcal{A}$ *there exists an adversary* $\mathcal{B}$ *with*

$$\left|\Pr\left[\mathsf{G}_2^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_3^{\mathcal{A}} \Rightarrow 1\right]\right| \leq \mathsf{Adv}^{\mathsf{uss}}_{\Pi}(\mathcal{B}) + Q_d\mathsf{uncert}(\mathcal{A})$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c + Q_d) \cdot \mathsf{poly}(\lambda)$.

Proof. A difference between G_2 and G_3 occurs iff the adversary issues a Dec query with $(\mathsf{id}, \mathsf{C} = (\pi, [\mathbf{c}_0]_1, [\mathbf{c}_1]_1), \mathsf{pred})$ where $(\mathsf{id}, \mathsf{C}) \notin \mathcal{C}_{\mathsf{enc}}$ and $\mathbf{c}_0 \notin \mathsf{Span}(\mathbf{A})$, but still $\mathsf{Ver}_{\mathsf{NIZK}}(\mathsf{crs}, [\mathbf{c}_1]_1, [\mathbf{c}_0]_1, \pi) = 1$ and $\mathsf{pred}(\mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id}, \mathsf{C})) = 1$ for a valid user secret key $\mathsf{usk}[\mathsf{id}]$ for id. In this case, however, the adversary can be used to break the USS property of Π: The reduction can use the Sim oracle to compute the QANIZK proofs in the Enc queries. When the adversary issues the Dec query with $(\mathsf{id}, \mathsf{C} = (\pi, [\mathbf{c}_0]_1, [\mathbf{c}_1]_1), \mathsf{pred})$ that satisfies the above properties, we have to distinguish the following two cases:



INIT:
$\mathcal{PG} \xleftarrow{\$} \mathsf{PGGen}(1^\lambda)$
parse $\mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
$\mathsf{sk}_{\mathsf{MAC}} \xleftarrow{\$} \mathsf{Gen}_{\mathsf{MAC}}(\mathbb{G}_2, q, P_2)$
$\mathsf{sk}_{\mathsf{MAC}} =: \big(\mathbf{B}, (\mathbf{X}_{i,j})_{1\le i\le L, 1\le j\le \ell'(i)}, \mathbf{x}'\big)$
$\mathbf{A} \xleftarrow{\$} \mathcal{D}_{k+\eta,k}$ s.t. $\overline{\mathbf{A}}$ has full rank.
$(\mathsf{crs}, \mathsf{td}) \xleftarrow{\$} \mathsf{Gen}_{\mathsf{crs}}(\mathcal{PG}, \mathbf{A})$
for $i \in \{1, \dots, L\},\ j \in \{1, \dots, \ell'(i)\}$ **do**
  $\mathbf{Y}_{i,j} \xleftarrow{\$} \mathbb{Z}_q^{k\times n};\ \mathbf{Z}_{i,j} := \big(\mathbf{Y}_{i,j}^\top \mid \mathbf{X}_{i,j}^\top\big)\mathbf{A}$
$\mathbf{y}' \xleftarrow{\$} \mathbb{Z}_q^k;\ \mathbf{z}' := \big(\mathbf{y}'^\top \mid \mathbf{x}'^\top\big) \cdot \mathbf{A}$
$\widetilde{\mathbf{Z}} := \big([\mathbf{Z}_{i,j}]_1\big)_{1\le i\le L, 1\le j\le \ell'(i)}$
return $\big(\mathsf{crs}, \mathcal{PG}, [\mathbf{A}]_1, \widetilde{\mathbf{Z}}, [\mathbf{z}']_1\big)$

EXT($\mathsf{id} \in \mathcal{S}^p$):
$\mathcal{Q}_{\mathcal{ID}} := \mathcal{Q}_{\mathcal{ID}} \cup \{\mathsf{id}\}$; **return** $\mathsf{Ext}'(\mathsf{id})$

$\mathsf{Ext}'(\mathsf{id} \in \mathcal{S}^p)$:
$\big([\mathbf{t}]_2, [\mathbf{u}]_2\big) \xleftarrow{\$} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{id})$
$\mathbf{S} \xleftarrow{\$} \mathsf{GL}_{n'}(\mathbb{Z}_q);\ \mathbf{T} := \mathbf{B} \cdot \mathbf{S}$
$\mathbf{U} := \sum_{i=1}^{p}\sum_{j=1}^{\ell'(i)} f_{i,j}\big(\mathsf{m}_{|i}\big)\mathbf{X}_{i,j}\mathbf{T}$
$\mathbf{v} := \sum_{i=1}^{p}\sum_{j=1}^{\ell'(i)} f_{i,j}\big(\mathsf{id}_{|i}\big)\mathbf{Y}_{i,j}\mathbf{t} + \mathbf{y}'$
$\mathbf{V} := \sum_{i=1}^{p}\sum_{j=1}^{\ell'(i)} f_{i,j}\big(\mathsf{id}_{|i}\big)\mathbf{Y}_{i,j}\mathbf{T}$
$\mathbf{v}^\top := \Big(\mathbf{t}^\top \sum_{i=1}^{p}\sum_{j=1}^{\ell'(i)} f_{i,j}\big(\mathsf{id}_{|i}\big)\mathbf{Z}_{i,j} + \mathbf{z}' - \mathbf{u}^\top\underline{\mathbf{A}}\Big)\overline{\mathbf{A}}^{-1}$
$\mathbf{V}^\top := \Big(\mathbf{T}^\top \sum_{i=1}^{p}\sum_{j=1}^{\ell'(i)} f_{i,j}\big(\mathsf{id}_{|i}\big)\mathbf{Z}_{i,j} - \mathbf{U}^\top\underline{\mathbf{A}}\Big)\overline{\mathbf{A}}^{-1}$
for $i \in \{p+1, \dots, L\},\ j \in \{1, \dots, \ell'(i)\}$ **do**
  $\mathbf{d}_{i,j} := \mathbf{X}_{i,j}\mathbf{t};\ \mathbf{D}_{i,j} := \mathbf{X}_{i,j}\mathbf{T}$
  $\mathbf{e}_{i,j} := \mathbf{Y}_{i,j}\mathbf{t};\ \mathbf{E}_{i,j} := \mathbf{Y}_{i,j}\mathbf{T}$
  $\mathbf{e}_{i,j}^\top := \big(\mathbf{t}^\top\mathbf{Z}_{i,j} - \mathbf{d}_{i,j}^\top\underline{\mathbf{A}}\big)\overline{\mathbf{A}}^{-1}$
  $\mathbf{E}_{i,j}^\top := \big(\mathbf{T}^\top\mathbf{Z}_{i,j} - \mathbf{D}_{i,j}^\top\underline{\mathbf{A}}\big)\overline{\mathbf{A}}^{-1}$
$\mathsf{usk}[\mathsf{id}] := \big([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{v}]_2\big)$
$\mathsf{udk}_1[\mathsf{id}] := \big([\mathbf{T}]_2, [\mathbf{U}]_2, [\mathbf{V}]_2\big)$
$\mathsf{udk}_2[\mathsf{id}] := \big([\mathbf{d}_{i,j}]_2, [\mathbf{D}_{i,j}]_2, [\mathbf{e}_{i,j}]_2, [\mathbf{E}_{i,j}]_2\big)_{p+1\le i\le L, 1\le j\le \ell'(i)}$
return $(\mathsf{usk}[\mathsf{id}], (\mathsf{udk}_1[\mathsf{id}], \mathsf{udk}_2[\mathsf{id}]))$

ENC($\mathsf{id}_0^\star \in \mathcal{S}^{p_0}, \mathsf{id}_1^\star \in \mathcal{S}^{p_1}$):
$\mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^k;\ \mathbf{c}_0^\star := \mathbf{A}\mathbf{r};$ $\mathbf{c}_0^\star \xleftarrow{\$} \mathbb{Z}_q^{k+\eta}$
$\mathbf{h} \xleftarrow{\$} \mathbb{Z}_q^\eta;\ \overline{\mathbf{c}_0^\star} \xleftarrow{\$} \mathbb{Z}_q^k;\ \underline{\mathbf{c}_0^\star} := \mathbf{h} + \underline{\mathbf{A}} \cdot \overline{\mathbf{A}}^{-1}\overline{\mathbf{c}_0^\star}$
$\mathbf{c}_1^\star := \sum_{i=1}^{p_0}\sum_{j=1}^{\ell'(i)} f_{i,j}\big((\mathsf{id}_0^\star)_{|i}\big)\mathbf{Z}_{i,j}\mathbf{r}$
$\mathbf{c}_1^\star := \sum_{i=1}^{p_0}\sum_{j=0}^{\ell'(i)}\big(f_{i,j}\big((\mathsf{id}_0^\star)_{|i}\big)\big(\mathbf{Y}_{i,j}^\top \mid \mathbf{X}_{i,j}^\top\big)\big)\mathbf{c}_0^\star$
$\mathbf{c}_1^\star := \sum_{i=1}^{p_0}\sum_{j=0}^{\ell'(i)}\Big(f_{i,j}\big((\mathsf{id}_0^\star)_{|i}\big)\Big(\mathbf{Z}_{i,j}\overline{\mathbf{A}}^{-1}\overline{\mathbf{c}_0^\star} + \mathbf{X}_{i,j}^\top\mathbf{h}\Big)\Big)$
$\mathbf{c}_1 \xleftarrow{\$} \mathbb{Z}_q^n;\ \pi \xleftarrow{\$} \mathsf{Prove}\big(\mathsf{crs}, [\mathbf{c}_1]_1, [\mathbf{c}_0]_1, \mathbf{r}\big)$
$\pi \xleftarrow{\$} \mathsf{Sim}\big(\mathsf{crs}, \mathsf{td}, [\mathbf{c}_1]_1, [\mathbf{c}_0]_1\big)$
$\mathsf{C}^\star := \big(\pi, [\mathbf{c}_0^\star]_1, [\mathbf{c}_1^\star]_1\big)$
$\mathcal{C}_{\mathsf{enc}} := \mathcal{C}_{\mathsf{enc}} \cup \{(\mathsf{id}_0^\star, \mathsf{C}^\star), (\mathsf{id}_1^\star, \mathsf{C}^\star)\}$
$\mathsf{K}^\star := \mathbf{z}' \cdot \mathbf{r};$ $\mathsf{K}^\star := \big(\mathbf{y}'^\top \mid \mathbf{x}'^\top\big)\mathbf{c}_0^\star$
$\mathsf{K}^\star := \mathbf{z}'\overline{\mathbf{A}}^{-1}\overline{\mathbf{c}_0^\star} + \mathbf{x}'^\top\mathbf{h};$ $\mathsf{K}^\star \xleftarrow{\$} \mathbb{Z}_q$
return $\big([\mathsf{K}^\star]_T, \mathsf{C}^\star\big)$

DEC($\mathsf{id} \in \mathcal{S}^p, \mathsf{C}, \mathsf{pred}$):
parse $\mathsf{C} =: \Big([\mathbf{c}_0]_1, \big([\mathbf{c}_1]_1\big)_{1\le\le\ell(p)}, \pi\Big)$
if $\mathsf{Ver}_{\mathsf{NIZK}}\big(\mathsf{crs}, [\mathbf{c}_1]_1, [\mathbf{c}_0]_1, \pi\big) = 0 \vee (\mathsf{id}, \mathsf{C}) \in \mathcal{C}_{\mathsf{enc}}$ **then return** $\bot$
if $\mathbf{c}_0 \notin \mathsf{Span}(\mathbf{A})$ **then return** $\bot$
if $\mathbf{c}_1 \neq \sum_{i=1}^{p}\sum_{j=1}^{\ell'(i)} f_{i,j}\big(\mathsf{id}_{|i}\big)\mathbf{Z}_{i,j}\overline{\mathbf{A}}^{-1}\overline{\mathbf{c}_0}$ **then**
return $\bot$
else
  $\mathsf{K} := \mathbf{z}'\overline{\mathbf{A}}^{-1}\overline{\mathbf{c}_0}$
  if $\mathsf{pred}\big([\mathsf{K}]_T\big) = 1$ **then return** $[\mathsf{K}]_T$
  else return $\bot$
$\big(\big([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{v}]_2\big), \mathsf{udk}[\mathsf{id}]\big) \xleftarrow{\$} \mathsf{Ext}'(\mathsf{id})$
$[\mathsf{K}]_T := e\Big(\big[\mathbf{c}_0^\top\big]_1, \begin{bmatrix}\mathbf{v}\\ \mathbf{u}\end{bmatrix}_2\Big) - e\big(\big[\mathbf{c}_1^\top\big]_1, [\mathbf{t}]_2\big)$
if $\mathsf{pred}\big([\mathsf{K}]_T\big) = 1$ **then return** $[\mathsf{K}]_T$ **else return** $\bot$

FINALIZE($\beta \in \{0, 1\}$):
return $\big(\bigcup_{(\mathsf{id}^\star, \mathsf{C}^\star)\in\mathcal{C}_{\mathsf{enc}}} \mathsf{Prefix}(\mathsf{id}^\star) \cap \mathcal{Q}_{\mathcal{ID}} = \emptyset\big) \wedge \beta$

Fig. 36. Hybrids for the security proof of the $\mathsf{AHIBKEM}_{\mathsf{CCA}}$ transformation. Ext' is just a helper function, not an oracle for the adversary.

– The ciphertext C was returned by the ENC oracle before for an identity $\mathsf{id}^\star \neq \mathsf{id}$. (If $\mathsf{id} = \mathsf{id}^\star$, the DEC query would not be allowed.) Let $([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{v}]_2)$ be a user secret key for id. Then

$$\begin{aligned}\mathsf{K} &= \mathbf{c}_0^\top \begin{pmatrix}\mathbf{v}\\ \mathbf{u}\end{pmatrix} - \mathbf{c}_1^\top \mathbf{t} \\ &= \mathbf{c}_0^\top \left(\sum_{i=1}^{p} \sum_{j=1}^{\ell'(i)} f_{i,j}\big(\mathsf{id}_{|i}\big) \begin{pmatrix}\mathbf{Y}_{i,j}\\ \mathbf{X}_{i,j}\end{pmatrix} \mathbf{t} + \begin{pmatrix}\mathbf{y}'\\ \mathbf{x}'\end{pmatrix} \right) - \mathbf{c}_0^\top \sum_{i=1}^{p} \sum_{j=1}^{\ell'(i)} f_{i,j}\Big(\mathsf{id}^\star_{|i}\Big) \begin{pmatrix}\mathbf{Y}_{i,j}\\ \mathbf{X}_{i,j}\end{pmatrix} \mathbf{t} \\ &= \mathbf{c}_0^\top \begin{pmatrix}\mathbf{y}'\\ \mathbf{x}'\end{pmatrix} + \mathbf{c}_0^\top \sum_{i=1}^{p} \sum_{j=1}^{\ell'(i)} \Big(f_{i,j}\big(\mathsf{id}_{|i}\big) - f_{i,j}\Big(\mathsf{id}^\star_{|i}\Big) \Big) \begin{pmatrix}\mathbf{X}_{i,j}\\ \mathbf{Y}_{i,j}\end{pmatrix} \mathbf{t} \,. \end{aligned}$$

Assume $\sum_{i=1}^{p} \sum_{j=1}^{\ell'(i)} \Big(f_{i,j}\big(\mathsf{id}_{|i}\big) - f_{i,j}\Big(\mathsf{id}^\star_{|i}\Big) \Big) \neq 0$ – if this would not be the case, the underlying affine MAC with levels could be trivially broken. Since $\mathbf{t}$ is a uniform random vector, K is uniformly random to the adversary. Thus DEC queries of this type are rejected due to $\mathsf{pred}([\mathsf{K}]_T) = 0$ anyway with probability at least $(1 - Q_d \mathsf{uncert}(\mathcal{A}))$. So in this case the adversary will not notice any difference between G_2 and G_3 for these queries.

– The ciphertext C was not returned by the ENC oracle before. In this case the ciphertext can be send to the $\textsc{Finalize}_{\mathsf{NIZK}}$ oracle to win the USS game.

□

Lemma 77 ($\mathsf{G}_3 \rightsquigarrow \mathsf{G}_4$)**.**

$$\big|\Pr\big[\mathsf{G}_3^{\mathcal{A}} \Rightarrow 1\big] - \Pr\big[\mathsf{G}_4^{\mathcal{A}} \Rightarrow 1\big]\big| \leq Q_d \mathsf{uncert}(\mathcal{A})$$

Proof. A difference between G_3 and G_4 occurs iff the adversary issues a DEC query with $(\mathsf{id}, \mathsf{C} = (\pi, [\mathbf{c}_0]_1, [\mathbf{c}_1]_1), \mathsf{pred})$ where $(\mathsf{id}, \mathsf{C}) \notin \mathcal{C}_{\mathsf{enc}}$, $\mathbf{c}_0 \in \mathsf{Span}(\mathbf{A})$, and $\mathbf{c}_1 \neq \sum_{i=1}^{p} \sum_{j=1}^{\ell'(i)} f_{i,j}\big(\mathsf{id}_{|i}\big) \mathbf{Z}_{i,j} \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}_0}$, but still $\mathsf{Ver}_{\mathsf{NIZK}}(\mathsf{crs}, [\mathbf{c}_1]_1, [\mathbf{c}_0]_1, \pi) = 1$ and $\mathsf{pred}(\mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id}, \mathsf{C})) = 1$ for a valid user secret key $\mathsf{usk}[\mathsf{id}]$ for id. Let $([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{v}]_2)$ be a user secret key for id. Then

$$\begin{aligned}\mathsf{K} &= \mathbf{c}_0^\top \begin{pmatrix}\mathbf{v}\\ \mathbf{u}\end{pmatrix} - \mathbf{c}_1^\top \mathbf{t} \\ &= \mathbf{c}_0^\top \left(\sum_{i=1}^{p} \sum_{j=1}^{\ell'(i)} f_{i,j}\big(\mathsf{id}_{|i}\big) \begin{pmatrix}\mathbf{Y}_{i,j}\\ \mathbf{X}_{i,j}\end{pmatrix} \mathbf{t} + \begin{pmatrix}\mathbf{y}'\\ \mathbf{x}'\end{pmatrix} \right) - \mathbf{c}_1^\top \mathbf{t} \\ &\overset{(*)}{=} \mathbf{c}_0^\top \begin{pmatrix}\mathbf{y}'\\ \mathbf{x}'\end{pmatrix} + \underbrace{\left(\overline{\mathbf{c}_0}^\top \overline{\mathbf{A}}^{-\top} \sum_{i=1}^{p} \sum_{j=1}^{\ell'(i)} f_{i,j}\big(\mathsf{id}_{|i}\big) \mathbf{Z}_{i,j}^\top - \mathbf{c}_1^\top \right)}_{=:\Delta} \mathbf{t} \,. \end{aligned}$$

In step $(*)$ we use that $\mathbf{c}_0 \in \mathsf{Span}(\mathbf{A})$. A DEC query with the properties from above has $\Delta \neq \mathbf{0}$. Since $\mathbf{t}$ is uniformly random to the adversary, $\mathsf{pred}([\mathsf{K}]_T)$ can output 1 only with probability at most $Q_d \mathsf{uncert}(\mathcal{A})$.

In G_4 all Dec queries are answered without using a user secret key for the queried identity. □

Lemma 78 ($\mathsf{G}_4 \rightsquigarrow \mathsf{G}_5$)**.**

$$\left|\Pr\left[\mathsf{G}_4^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_5^{\mathcal{A}} \Rightarrow 1\right]\right| \leq \frac{1}{q-1}$$

Proof. The proof is identical to Lemma 72. □

Lemma 79 ($\mathsf{G}_5 \rightsquigarrow \mathsf{G}_6$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}_5^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_6^{\mathcal{A}} \Rightarrow 1\right]\right| \leq \mathsf{Adv}^{\mathsf{mhpr\text{-}cma}}_{\mathsf{MAC},\mathsf{PGGen}}(\mathcal{B})$$

and $T(\mathcal{B}) \approx T(\mathcal{A}) + (Q_e + Q_c + Q_d) \cdot \mathsf{poly}(\lambda)$.

Proof. The proof is identical to Lemma 73. In G_6 $\mathsf{C}^\star$ is information-theoretically independent of the challenge identity. □

Summary. To prove Theorem 17, we combine Lemmas 74–79 to change the challenge keys $\mathsf{K}^\star$ and the challenge identities from $\mathsf{id}_0^\star$ to $\mathsf{id}_1^\star$ and then apply all Lemmata (except Lemma 79) in reverse order to get to the $\mathsf{mIND\text{-}AHID\text{-}CCCA}_1$ game. □

F Instantiations

F.1 MDDH

The result of applying the HIBKEM transformation to MAC_1 is shown in Figure 37. The scheme has $5\alpha\big(L^2+L\big)k^2+5k^2+k$ group elements in the master public key (including the delegation key) and $5k$ group elements in the ciphertext. The user secret keys (including the delegation key) have at most $2\alpha\big(L^2+L-2\big)k+5k$ group elements. Identities that are deeper in the hierarchy have smaller secret keys since the size of the delegation keys dominates the user secret key size. On the last level, the user secret keys consist of only $5k$ group elements. The scheme is IND-HID-CPA secure under the $\mathcal{U}_k$-MDDH assumption for pairing groups.

The result of applying the $\mathsf{HIBKEM}_{\mathsf{CPA}}$ transformation to MAC_2 is shown in Figure 38. The scheme has $5\alpha\big(L^2+L\big)k^2+5k^2+k$ group elements in the master public key (including the delegation key). Ciphertext and user secret keys both have at most $3Lk+2k$ group elements. Identities that are deeper in the hierarchy have larger secret keys and require larger ciphertexts. The scheme is IND-HID-CPA secure under the $\mathcal{U}_k$-MDDH assumption for pairing groups.

The schemes have both the same public key. The first scheme has smaller ciphertexts, while the second has smaller user secret keys in the worst case.

The result of applying the AHIBKEM transformation to MAC_1 is shown in Figure 39. The scheme has $3\alpha\big(L^2+L\big)k^2+2k^2+k$ group elements in the master public key (including the delegation key) and $5k$ group elements in the ciphertext. The user secret keys (including the delegation key) have at most

$\underline{\mathsf{Gen}(1^\lambda):}$
$\mathcal{PG} \xleftarrow{\$} \mathsf{PGGen}(1^\lambda)$
parse $\mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
$\mathbf{B} \xleftarrow{\$} \mathcal{U}_{3k,k}$; $\mathbf{A} \xleftarrow{\$} \mathcal{U}_{2k,k}$
for $i \in \{1,\dots,L\}$, $j \in \{1,\dots,i\alpha\}$, $b \in \{0,1\}$ **do**
  $\mathbf{X}_{i,j,b} \xleftarrow{\$} \mathbb{Z}_q^{k\times 3k}$; $\mathbf{Y}_{i,j,b} \xleftarrow{\$} \mathbb{Z}_q^{k\times 3k}$
  $\mathbf{Z}_{i,j,b} := \left(\mathbf{Y}_{i,j,b}^\top \mid \mathbf{X}_{i,j,b}^\top\right)\mathbf{A}$
  $\mathbf{D}_{i,j,b} := \mathbf{X}_{i,j,b} \cdot \mathbf{B}$; $\mathbf{E}_{i,j,b} := \mathbf{Y}_{i,j,b} \cdot \mathbf{B}$
$\mathbf{x}' \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{y}' \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{z}' := \left(\mathbf{y}'^\top \mid \mathbf{x}'^\top\right) \cdot \mathbf{A}$
$\widetilde{\mathbf{Z}} := \left(\left[\mathbf{Z}_{i,j,b}\right]_1\right)_{1\le i\le L, 1\le j\le i\alpha, b\in\{0,1\}}$
$\mathsf{pk} := \left(\mathcal{PG}, [\mathbf{A}]_1, \widetilde{\mathbf{Z}}, [\mathbf{z}']_1\right)$
$\widetilde{\mathsf{dk}} := \left(\left[\mathbf{D}_{i,j,b}\right]_2, \left[\mathbf{E}_{i,j,b}\right]_2\right)_{\substack{1\le i\le L, b\in\{0,1\},\\ 1\le j\le i\alpha}}$
$\mathsf{dk} := \left([\mathbf{B}]_2, \widetilde{\mathsf{dk}}\right)$
$\mathsf{sk} := \left(\mathsf{sk}_{\mathsf{MAC}}, \left(\mathbf{Y}_{i,j,b}\right)_{\substack{1\le i\le L, b\in\{0,1\},,\\ 1\le j\le i\alpha}}, \mathbf{y}'\right)$
return $(\mathsf{pk}, \mathsf{dk}, \mathsf{sk})$

$\underline{\mathsf{Enc}(\mathsf{pk}, \mathsf{id} \in \mathcal{S}^p):}$
$\mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{c}_0 := \mathbf{A}\mathbf{r}$
$\mathbf{c}_1 := \sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{Z}_{i,j,[\![\mathsf{id}]\!]_j}\mathbf{r}$
$\mathsf{C} := \left([\mathbf{c}_0]_1, [\mathbf{c}_1]_1\right)$
$\mathsf{K} := \mathbf{z}' \cdot \mathbf{r}$
return $\left([\mathsf{K}]_T, \mathsf{C}\right)$

$\underline{\mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id} \in \mathcal{S}^p, \mathsf{C}):}$
parse $\mathsf{usk}[\mathsf{id}] =: \left([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$
parse $\mathsf{C} =: \left([\mathbf{c}_0]_1, [\mathbf{c}_1]_1\right)$
$[\mathsf{K}]_T := \left[\mathbf{c}_0^\top\right]_1 \circ \begin{bmatrix}\mathbf{v}\\ \mathbf{u}\end{bmatrix}_2 - \left[\mathbf{c}_1^\top\right]_1 \circ [\mathbf{t}]_2$
return $[\mathsf{K}]_T$

$\underline{\mathsf{Ext}(\mathsf{sk}, \mathsf{id} \in \mathcal{S}^p):}$
$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{t} := \mathbf{B}\mathbf{s}$
$\mathbf{u} := \sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{X}_{i,j,[\![\mathsf{id}]\!]_j}\mathbf{t} + \mathbf{x}'$
$\mathbf{v} := \sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{Y}_{i,j,[\![\mathsf{id}]\!]_j}\mathbf{t} + \mathbf{y}'$
for $i \in \{p+1,\dots,L\}$, $j \in \{1,\dots,i\alpha\}$, $b \in \{0,1\}$ **do**
  $\mathbf{d}_{i,j,b} := \mathbf{X}_{i,j,b}\mathbf{t}$; $\mathbf{e}_{i,j,b} := \mathbf{Y}_{i,j,b}\mathbf{t}$
$\mathsf{usk}[\mathsf{id}] := \left([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$
$\mathsf{udk}[\mathsf{id}] := \left([\mathbf{d}_{i,j,b}]_2, [\mathbf{e}_{i,j,b}]_2\right)_{\substack{p+1\le i\le L,\\ 1\le j\le i\alpha,\\ b\in\{0,1\}}}$
return $(\mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}])$

$\underline{\mathsf{Del}(\mathsf{dk}, \mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}], \mathsf{id} \in \mathcal{S}^p, \mathsf{id}_{p+1}):}$
parse $\mathsf{usk} =: \left([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$
$\mathbf{s}' \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{t}' := \mathbf{t} + \mathbf{B}\mathbf{s}'$
$\mathsf{id}' := (\mathsf{id}_1, \dots, \mathsf{id}_p, \mathsf{id}_{p+1})$
$\mathbf{u}' := \mathbf{u} + \sum_{j=1}^{(p+1)\alpha} \mathbf{d}_{p+1,j,[\![\mathsf{id}']\!]_j} + \sum_{i=1}^{p+1}\sum_{j=1}^{i\alpha} \mathbf{D}_{i,j,[\![\mathsf{id}']\!]_j}\mathbf{s}'$
$\mathbf{v}' := \mathbf{v} + \sum_{j=1}^{(p+1)\alpha} \mathbf{e}_{p+1,j,[\![\mathsf{id}']\!]_j} + \sum_{i=1}^{p+1}\sum_{j=1}^{i\alpha} \mathbf{E}_{i,j,[\![\mathsf{id}']\!]_j}\mathbf{s}'$
for $i \in \{p+2,\dots,L\}$, $j \in \{1,\dots,i\alpha\}$, $b \in \{0,1\}$ **do**
  $\mathbf{d}'_{i,j,b} := \mathbf{d}_{i,j,b} + \mathbf{D}_{i,j,b}\mathbf{s}'$
  $\mathbf{e}'_{i,j,b} := \mathbf{e}_{i,j,b} + \mathbf{E}_{i,j,b}\mathbf{s}'$
$\mathsf{usk}[\mathsf{id}'] := \left([\mathbf{t}']_2, [\mathbf{u}']_2, [\mathbf{v}']_2\right)$
$\mathsf{udk}[\mathsf{id}'] := \left(\left[\mathbf{d}'_{i,j,b}\right]_2, \left[\mathbf{e}'_{i,j,b}\right]_2\right)_{\substack{p+2\le i\le L,\\ 1\le j\le i\alpha,\\ b\in\{0,1\}}}$
return $(\mathsf{usk}[\mathsf{id}'], \mathsf{udk}[\mathsf{id}'])$

Fig. 37. The resulting scheme $\mathsf{HIBKEM}_1 := \mathsf{HIBKEM}_{\mathsf{CPA}}[\mathsf{MAC}_1, \mathcal{U}_{2k,k}]$.

$\underline{\mathsf{Gen}\left(1^\lambda\right)\text{:}}$
$\mathcal{PG} \xleftarrow{\$} \mathsf{PGGen}\left(1^\lambda\right)$
parse $\mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
$\mathbf{B} \xleftarrow{\$} \mathcal{U}_{3k,k}$; $\mathbf{A} \xleftarrow{\$} \mathcal{U}_{2k,k}$
for $i \in \{1, \dots, L\}$, $j \in \{1, \dots, i\alpha\}$, $b \in \{0,1\}$ **do**
  $\mathbf{X}_{i,j,b} \xleftarrow{\$} \mathbb{Z}_q^{k \times 3k}$; $\mathbf{Y}_{i,j,b} \xleftarrow{\$} \mathbb{Z}_q^{k \times 3k}$
  $\mathbf{Z}_{i,j,b} := \left(\mathbf{Y}_{i,j,b}^\top \mid \mathbf{X}_{i,j,b}^\top\right)\mathbf{A}$
  $\mathbf{D}_{i,j,b} := \mathbf{X}_{i,j,b} \cdot \mathbf{B}$; $\mathbf{E}_{i,j,b} := \mathbf{Y}_{i,j,b} \cdot \mathbf{B}$
$\mathbf{x}' \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{y}' \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{z}' := \left(\mathbf{y}'^\top \mid \mathbf{x}'^\top\right) \cdot \mathbf{A}$
$\widetilde{\mathbf{Z}} := \left(\left[\mathbf{Z}_{i,j,b}\right]_1\right)_{1 \le i \le L, 1 \le j \le i\alpha, b \in \{0,1\}}$
$\mathsf{pk} := \left(\mathcal{PG}, [\mathbf{A}]_1, \widetilde{\mathbf{Z}}, [\mathbf{z}']_1\right)$
$\widetilde{\mathsf{dk}} := \left(\left[\mathbf{D}_{i,j,b}\right]_2, \left[\mathbf{E}_{i,j,b}\right]_2\right)_{\substack{1 \le i \le L, b \in \{0,1\}, \\ 1 \le j \le i\alpha}}$
$\mathsf{dk} := \left([\mathbf{B}]_2, \widetilde{\mathsf{dk}}\right)$
$\mathsf{sk} := \left(\mathsf{sk}_{\mathsf{MAC}}, \left(\mathbf{Y}_{i,j,b}\right)_{\substack{1 \le i \le L, b \in \{0,1\}, \\ 1 \le j \le i\alpha}}, \mathbf{y}'\right)$
return $(\mathsf{pk}, \mathsf{dk}, \mathsf{sk})$

$\underline{\mathsf{Ext}(\mathsf{sk}, \mathsf{id} \in \mathcal{S}^p)\text{:}}$
for $i \in \{1, \dots, p\}$ **do** $\mathbf{s}_i \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{t}_i := \mathbf{B}\mathbf{s}_i$
$\mathbf{u} := \sum_{i=1}^{p} \sum_{j=1}^{i\alpha} \mathbf{X}_{i,j,[\![\mathsf{m}]\!]_j} \mathbf{t}_i + \mathbf{x}'$
$\mathbf{v} := \sum_{i=1}^{p} \sum_{j=1}^{i\alpha} \mathbf{Y}_{i,j,[\![\mathsf{id}]\!]_j} \mathbf{t}_i + \mathbf{y}'$
return $\left(\left([\mathbf{t}_i]_2\right)_{1 \le i \le p}, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$

$\underline{\mathsf{Del}(\mathsf{dk}, \mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}], \mathsf{id} \in \mathcal{S}^p, \mathsf{id}_{p+1})\text{:}}$
parse $\mathsf{usk}[\mathsf{id}] =: \left(\left([\mathbf{t}_i]_2\right)_{1 \le i \le p}, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$
for $i \in \{1, \dots, p\}$ **do**
  $\mathbf{s}_i' \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{t}_i' := \mathbf{t}_i + \mathbf{B}\mathbf{s}_i'$
$\mathbf{s}_{p+1}' \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{t}_{p+1}' := \mathbf{B}\mathbf{s}_{p+1}'$
$\mathsf{id}' := (\mathsf{id}_1, \dots, \mathsf{id}_p, \mathsf{id}_{p+1})$
$\mathbf{u}' := \mathbf{u} + \sum_{i=1}^{p+1} \sum_{j=1}^{i\alpha} \mathbf{D}_{i,j,[\![\mathsf{id}']\!]_j} \mathbf{s}_i'$
$\mathbf{v}' := \mathbf{v} + \sum_{i=1}^{p+1} \sum_{j=1}^{i\alpha} \mathbf{E}_{i,j,[\![\mathsf{id}']\!]_j} \mathbf{s}_i'$
return $\left(\left([\mathbf{t}']_2\right)_{1 \le i \le p+1}, [\mathbf{u}']_2, [\mathbf{v}']_2\right)$

$\underline{\mathsf{Enc}(\mathsf{pk}, \mathsf{id} \in \mathcal{S}^p)\text{:}}$
$\mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{c}_0 := \mathbf{A}\mathbf{r}$
for $i \in \{1, \dots, p\}$ **do**
  $\mathbf{c}_{1,i} := \sum_{j=1}^{i\alpha} \mathbf{Z}_{i,j,[\![\mathsf{id}]\!]_j} \mathbf{r}$
$\mathsf{C} := \left(\left[\mathbf{c}_0\right]_1, \left(\left[\mathbf{c}_{1,i}\right]_1\right)_{1 \le i \le p}\right)$
$\mathsf{K} := \mathbf{z}' \cdot \mathbf{r}$
return $\left([\mathsf{K}]_T, \mathsf{C}\right)$

$\underline{\mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id} \in \mathcal{S}^p, \mathsf{C})\text{:}}$
parse $\mathsf{usk}[\mathsf{id}] =: \left(\left([\mathbf{t}_i]_2\right)_{1 \le i \le p}, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$
parse $\mathsf{C} =: \left(\left[\mathbf{c}_0\right]_1, \left(\left[\mathbf{c}_{1,i}\right]_1\right)_{1 \le i \le p}\right)$
$[\mathsf{K}]_T := \left[\mathbf{c}_0^\top\right]_1 \circ \begin{bmatrix}\mathbf{v}\\ \mathbf{u}\end{bmatrix}_2 - \sum_{i=1}^{p} \left(\left[\mathbf{c}_{1,i}^\top\right]_1 \circ [\mathbf{t}_i]_2\right)$
return $[\mathsf{K}]_T$

Fig. 38. The resulting scheme $\mathsf{HIBKEM}_2 := \mathsf{HIBKEM}_{\mathsf{CPA}}[\mathsf{MAC}_2, \mathcal{U}_{2k,k}]$.

$2\alpha\big(L^2+L-2\big)\big(k^2+k\big)+5k^2+5k$ group elements. Identities that are deeper in the hierarchy have smaller secret keys since the size of the delegation keys dominates the user secret key size. On the last level, the user secret keys consist of only $5k^2+5k$ group elements. The scheme is PR-HID-CPA secure under the $\mathcal{U}_k$-MDDH assumption for pairing groups.

F.2 SXDH

With a type III pairing, all of the schemes in this paper can be instantiated with the SXDH assumption.

The result (HIBKEM_1) of instantiating scheme $\mathsf{HIBKEM}_{\mathsf{CPA}}[\mathsf{MAC}_1,\mathcal{U}_{2k,k}]$ with the SXDH assumption is shown in Figure 40. The scheme has $5\alpha\big(L^2+L\big)+6$ group elements in the public key and 5 group elements in the ciphertext. The user secret keys have at most $2\alpha\big(L^2+L-2\big)+5$ group elements.

The result (HIBKEM_2) of instantiating scheme $\mathsf{HIBKEM}_{\mathsf{CPA}}[\mathsf{MAC}_2,\mathcal{U}_{2k,k}]$ with the SXDH assumption is shown in Figure 41. The scheme has $5\alpha\big(L^2+L\big)+6$ group elements in the public key and at most $3L+2$ group elements in a ciphertext or a user secret key.

The result (HIBKEM_3) of instantiating scheme $\mathsf{AHIBKEM}_{\mathsf{CPA}}[\mathsf{MAC}_1,\mathcal{U}_{2k,k}]$ with the SXDH assumption is shown in Figure 42. The scheme has $3\alpha\big(L^2+L\big)+3$ group elements in the public key and 5 group elements in the ciphertext. The user secret keys have at most $4\alpha\big(L^2+L-2\big)+10$ group elements.

$\underline{\mathsf{Gen}(1^\lambda):}$
$\mathcal{PG} \xleftarrow{\$} \mathsf{PGGen}(1^\lambda)$
parse $\mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
$\mathsf{sk}_{\mathsf{MAC}} \xleftarrow{\$} \mathsf{Gen}_{\mathsf{MAC}}(\mathbb{G}_2, q, P_2)$
$\mathsf{sk}_{\mathsf{MAC}} =: \left(\mathbf{B}, \left(\mathbf{X}_{i,j,b}\right)_{\substack{1\le i\le L, b\in\{0,1\},\\ 1\le j\le i\alpha}}, \mathbf{x}'\right)$
$\mathbf{A} \xleftarrow{\$} \mathcal{U}_{2k,k}$
for $i \in \{1,\dots,L\},\ j \in \{1,\dots,i\alpha\},\ b \in \{0,1\}$ **do**
  $\mathbf{Y}_{i,j,b} \xleftarrow{\$} \mathbb{Z}_q^{k\times 3k}$
  $\mathbf{Z}_{i,j,b} := \left(\mathbf{Y}_{i,j,b}^\top \mid \mathbf{X}_{i,j,b}^\top\right)\mathbf{A}$
$\mathbf{y}' \xleftarrow{\$} \mathbb{Z}_q^k;\ \mathbf{z}' := \left(\mathbf{y}'^\top \mid \mathbf{x}'^\top\right)\cdot\mathbf{A}$
$\widetilde{\mathbf{Z}} := \left(\left[\mathbf{Z}_{i,j,b}\right]_1\right)_{1\le i\le L, 1\le j\le i\alpha, b\in\{0,1\}}$
$\mathsf{pk} := \left(\mathcal{PG}, [\mathbf{A}]_1, \widetilde{\mathbf{Z}}, [\mathbf{z}']_1\right)$
$\mathsf{sk} := \left(\mathsf{sk}_{\mathsf{MAC}}, \left(\mathbf{Y}_{i,j,b}\right)_{\substack{1\le i\le L, b\in\{0,1\},\\ 1\le j\le i\alpha}}, \mathbf{y}'\right)$
return $(\mathsf{pk}, \mathsf{sk})$

$\underline{\mathsf{Ext}(\mathsf{sk}, \mathsf{id} \in \mathcal{S}^p):}$
$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k;\ \mathbf{t} := \mathbf{B}\mathbf{s}$
$\mathbf{S} \xleftarrow{\$} \mathsf{GL}_k(\mathbb{Z}_q);\ \mathbf{T} := \mathbf{B}\cdot\mathbf{S}$
$\mathbf{u} := \sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{X}_{i,j,[\![\mathsf{id}]\!]_j}\mathbf{t} + \mathbf{x}'$
$\mathbf{U} := \sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{X}_{i,j,[\![\mathsf{id}]\!]_j}\mathbf{T}$
$\mathbf{v} := \sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{Y}_{i,j,[\![\mathsf{id}]\!]_j}\mathbf{t} + \mathbf{y}'$
$\mathbf{V} := \sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{Y}_{i,j,[\![\mathsf{id}]\!]_j}\mathbf{T}$
for $i \in \{p+1,\dots,L\},\ j \in \{1,\dots,i\alpha\},\ b \in \{0,1\}$ **do**
  $\mathbf{d}_{i,j,b} := \mathbf{X}_{i,j,b}\mathbf{t};\ \mathbf{D}_{i,j,b} := \mathbf{X}_{i,j,b}\mathbf{T}$
  $\mathbf{e}_{i,j,b} := \mathbf{Y}_{i,j,b}\mathbf{t};\ \mathbf{E}_{i,j,b} := \mathbf{Y}_{i,j,b}\mathbf{T}$
$\mathsf{usk}[\mathsf{id}] := \left([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$
$\mathsf{udk}_1[\mathsf{id}] := \left([\mathbf{T}]_2, [\mathbf{U}]_2, [\mathbf{V}]_2\right)$
$\mathsf{udk}_2[\mathsf{id}] := \left(\left[\mathbf{d}_{i,j,b}\right]_2, \left[\mathbf{D}_{i,j,b}\right]_2, \left[\mathbf{e}_{i,j,b}\right]_2, \left[\mathbf{E}_{i,j,b}\right]_2\right)_{p+1\le i\le L, 1\le j\le i\alpha}$
return $(\mathsf{usk}[\mathsf{id}], (\mathsf{udk}_1[\mathsf{id}], \mathsf{udk}_2[\mathsf{id}]))$

$\underline{\mathsf{Del}(\mathsf{dk}, \mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}], \mathsf{id} \in \mathcal{S}^p, \mathsf{id}_{p+1}):}$
parse $\mathsf{usk}[\mathsf{id}] =: \left([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$
parse $\mathsf{udk}[\mathsf{id}] =: \left([\mathbf{T}]_2, [\mathbf{U}]_2, [\mathbf{V}]_2, \mathsf{udk}_2\right)$
parse $\mathsf{udk}_2 =: \left(\left[\mathbf{d}_{i,j,b}\right]_2, \left[\mathbf{D}_{i,j,b}\right]_2, \left[\mathbf{e}_{i,j,b}\right]_2, \left[\mathbf{E}_{i,j,b}\right]_2\right)_{p+1\le i\le L, 1\le j\le i\alpha}$
$\mathsf{id}' := (\mathsf{id}_1, \dots, \mathsf{id}_p, \mathsf{id}_{p+1})$
$\mathbf{u}' := \mathbf{u} + \sum_{j=1}^{(p+1)\alpha} \mathbf{d}_{p+1,j,[\![\mathsf{id}]\!]_j}$
$\mathbf{U}' := \mathbf{U} + \sum_{j=1}^{(p+1)\alpha} \mathbf{D}_{p+1,j,[\![\mathsf{id}]\!]_j}$
$\mathbf{v}' := \mathbf{v} + \sum_{j=1}^{(p+1)\alpha} \mathbf{e}_{p+1,j,[\![\mathsf{id}]\!]_j}$
$\mathbf{V}' := \mathbf{V} + \sum_{j=1}^{(p+1)\alpha} \mathbf{E}_{p+1,j,[\![\mathsf{id}]\!]_j}$
$\mathbf{s}' \xleftarrow{\$} \mathbb{Z}_q^k;\ \mathbf{t}' := \mathbf{t} + \mathbf{T}\cdot\mathbf{s}'$
$\mathbf{S}' \xleftarrow{\$} \mathsf{GL}_k(\mathbb{Z}_q);\ \mathbf{T}' := \mathbf{T}\mathbf{S}'$
$\mathbf{u}'' := \mathbf{u} + \mathbf{U}\mathbf{s}';\ \mathbf{v} := \mathbf{v} + \mathbf{V}\mathbf{s}'$
$\mathbf{U} := \mathbf{U}\cdot\mathbf{S}';\ \mathbf{V} := \mathbf{V}\cdot\mathbf{S}'$
for $i \in \{p+2,\dots,L\},\ j \in \{1,\dots,\ell'(i)\}$ **do**
  $\mathbf{d}'_{i,j,b} := \mathbf{d}_{i,j,b} + \mathbf{D}_{i,j,b}\mathbf{s}'$
  $\mathbf{e}'_{i,j,b} := \mathbf{e}_{i,j,b} + \mathbf{E}_{i,j,b}\mathbf{s}'$
  $\mathbf{D}'_{i,j,b} := \mathbf{D}\cdot\mathbf{S}';\ \mathbf{E}'_{i,j,b} := \mathbf{E}\cdot\mathbf{S}'$
$\mathsf{usk}[\mathsf{id}'] := \left([\mathbf{t}']_2, [\mathbf{u}'']_2, [\mathbf{v}'']_2\right)$
$\mathsf{udk}_1[\mathsf{id}'] := \left([\mathbf{T}']_2, [\mathbf{U}'']_2, [\mathbf{V}'']_2\right)$
$\mathsf{udk}_2[\mathsf{id}'] =: \left(\left[\mathbf{d}'_{i,j,b}\right]_2, \left[\mathbf{D}'_{i,j,b}\right]_2, \left[\mathbf{e}'_{i,j,b}\right]_2, \left[\mathbf{E}'_{i,j,b}\right]_2\right)_{p+1\le i\le L, 1\le j\le i\alpha}$
return $(\mathsf{usk}[\mathsf{id}'], \mathsf{udk}_1[\mathsf{id}'], \mathsf{udk}_2[\mathsf{id}'])$

$\underline{\mathsf{Enc}(\mathsf{pk}, \mathsf{id} \in \mathcal{S}^p):}$
$\mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^k;\ \mathbf{c}_0 := \mathbf{A}\mathbf{r}$
$\mathbf{c}_1 := \sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{Z}_{i,j,[\![\mathsf{id}]\!]_j}\mathbf{r}$
$\mathsf{C} := \left([\mathbf{c}_0]_1, [\mathbf{c}_1]_1\right)$
$\mathsf{K} := \mathbf{z}'\cdot\mathbf{r}$
return $\left([\mathsf{K}]_T, \mathsf{C}\right)$

$\underline{\mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id} \in \mathcal{S}^p, \mathsf{C}):}$
parse $\mathsf{usk}[\mathsf{id}] =: \left([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$
parse $\mathsf{C} =: \left([\mathbf{c}_0]_1, [\mathbf{c}_1]_1\right)$
$[\mathsf{K}]_T := e\left(\left[\mathbf{c}_0^\top\right]_1, \begin{bmatrix}\mathbf{v}\\ \mathbf{u}\end{bmatrix}_2\right) - e\left(\left[\mathbf{c}_1^\top\right]_1, [\mathbf{t}]_2\right)$
return $[\mathsf{K}]_T$

Fig. 39. The resulting scheme $\mathsf{HIBKEM}_3 := \mathsf{AHIBKEM}_{\mathsf{CPA}}[\mathsf{MAC}_1, \mathcal{U}_{2k,k}]$.

$\underline{\mathsf{Gen}\left(1^\lambda\right)}$:
$\mathcal{PG} \xleftarrow{\$} \mathsf{PGGen}\left(1^\lambda\right)$
parse $\mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
$\mathbf{B} \xleftarrow{\$} \mathcal{U}_{3,1}$; $\mathbf{A} \xleftarrow{\$} \mathcal{U}_1$
for $i \in \{1, \ldots, L\}$, $j \in \{1, \ldots, i\alpha\}$, $b \in \{0,1\}$ **do**
  $\mathbf{X}_{i,j,b} \xleftarrow{\$} \mathbb{Z}_q^{1\times 3}$; $\mathbf{Y}_{i,j,b} \xleftarrow{\$} \mathbb{Z}_q^{1\times 3}$
  $\mathbf{Z}_{i,j,b} := \left(\mathbf{Y}_{i,j,b}^\top \mid \mathbf{X}_{i,j,b}^\top\right)\mathbf{A}$
  $\mathbf{D}_{i,j,b} := \mathbf{X}_{i,j,b} \cdot \mathbf{B}$; $\mathbf{E}_{i,j,b} := \mathbf{Y}_{i,j,b} \cdot \mathbf{B}$
$\mathbf{x}' \xleftarrow{\$} \mathbb{Z}_q$; $\mathbf{y}' \xleftarrow{\$} \mathbb{Z}_q$; $\mathbf{z}' := (\mathbf{y}' \mid \mathbf{x}') \cdot \mathbf{A}$
$\widetilde{\mathbf{Z}} := \left(\left[\mathbf{Z}_{i,j,b}\right]_1\right)_{1\le i\le L, 1\le j\le i\alpha, b\in\{0,1\}}$
$\mathsf{pk} := \left(\mathcal{PG}, [\mathbf{A}]_1, \widetilde{\mathbf{Z}}, [\mathbf{z}']_1\right)$
$\widetilde{\mathsf{dk}} := \left(\left[\mathbf{D}_{i,j,b}\right]_2, \left[\mathbf{E}_{i,j,b}\right]_2\right)_{\substack{1\le i\le L, b\in\{0,1\},\\ 1\le j\le i\alpha}}$
$\mathsf{dk} := \left([\mathbf{B}]_2, \widetilde{\mathsf{dk}}\right)$
$\mathsf{sk} := \left(\mathsf{sk}_{\mathsf{MAC}}, \left(\mathbf{Y}_{i,j,b}\right)_{\substack{1\le i\le L, b\in\{0,1\},,\\ 1\le j\le i\alpha}}, \mathbf{y}'\right)$
return $(\mathsf{pk}, \mathsf{dk}, \mathsf{sk})$

$\underline{\mathsf{Enc}(\mathsf{pk}, \mathsf{id} \in \mathcal{S}^p)}$:
$\mathbf{r} \xleftarrow{\$} \mathbb{Z}_q$; $\mathbf{c}_0 := \mathbf{A}\mathbf{r}$
$\mathbf{c}_1 := \sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{Z}_{i,j,[\![\mathsf{id}]\!]_j}\mathbf{r}$
$\mathsf{C} := \left([\mathbf{c}_0]_1, [\mathbf{c}_1]_1\right)$
$\mathsf{K} := \mathbf{z}' \cdot \mathbf{r}$
return $\left([\mathsf{K}]_T, \mathsf{C}\right)$

$\underline{\mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id} \in \mathcal{S}^p, \mathsf{C})}$:
parse $\mathsf{usk}[\mathsf{id}] =: \left([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$
parse $\mathsf{C} =: \left([\mathbf{c}_0]_1, [\mathbf{c}_1]_1\right)$
$[\mathsf{K}]_T := \left[\mathbf{c}_0^\top\right]_1 \circ \begin{bmatrix}\mathbf{v}\\ \mathbf{u}\end{bmatrix}_2 - \left[\mathbf{c}_1^\top\right]_1 \circ [\mathbf{t}]_2$
return $[\mathsf{K}]_T$

$\underline{\mathsf{Ext}(\mathsf{sk}, \mathsf{id} \in \mathcal{S}^p)}$:
$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q$; $\mathbf{t} := \mathbf{B}\mathbf{s}$
$\mathbf{u} := \sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{X}_{i,j,[\![\mathsf{id}]\!]_j}\mathbf{t} + \mathbf{x}'$
$\mathbf{v} := \sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{Y}_{i,j,[\![\mathsf{id}]\!]_j}\mathbf{t} + \mathbf{y}'$
for $i \in \{p+1, \ldots, L\}$, $j \in \{1, \ldots, i\alpha\}$, $b \in \{0,1\}$ **do**
  $\mathbf{d}_{i,j,b} := \mathbf{X}_{i,j,b}\mathbf{t}$; $\mathbf{e}_{i,j,b} := \mathbf{Y}_{i,j,b}\mathbf{t}$
$\mathsf{usk}[\mathsf{id}] := \left([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$
$\mathsf{udk}[\mathsf{id}] := \left([\mathbf{d}_{i,j,b}]_2, [\mathbf{e}_{i,j,b}]_2\right)_{\substack{p+1\le i\le L,\\ 1\le j\le i\alpha,\\ b\in\{0,1\}}}$
return $(\mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}])$

$\underline{\mathsf{Del}(\mathsf{dk}, \mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}], \mathsf{id} \in \mathcal{S}^p, \mathsf{id}_{p+1})}$:
parse $\mathsf{usk} =: \left([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$
$\mathbf{s}' \xleftarrow{\$} \mathbb{Z}_q$; $\mathbf{t}' := \mathbf{t} + \mathbf{B}\mathbf{s}'$
$\mathsf{id}' := (\mathsf{id}_1, \ldots, \mathsf{id}_p, \mathsf{id}_{p+1})$
$\mathbf{u}' := \mathbf{u} + \sum_{j=1}^{(p+1)\alpha} \mathbf{d}_{p+1,j,[\![\mathsf{id}']\!]_j} + \sum_{i=1}^{p+1}\sum_{j=1}^{i\alpha} \mathbf{D}_{i,j,[\![\mathsf{id}']\!]_j}\mathbf{s}'$
$\mathbf{v}' := \mathbf{v} + \sum_{j=1}^{(p+1)\alpha} \mathbf{e}_{p+1,j,[\![\mathsf{id}']\!]_j} + \sum_{i=1}^{p+1}\sum_{j=1}^{\ell'(,i)} \mathbf{E}_{i,j,[\![\mathsf{id}']\!]_j}\mathbf{s}'$
for $i \in \{p+2, \ldots, L\}$, $j \in \{1, \ldots, i\alpha\}$, $b \in \{0,1\}$ **do**
  $\mathbf{d}'_{i,j,b} := \mathbf{d}_{i,j,b} + \mathbf{D}_{i,j,b}\mathbf{s}'$
  $\mathbf{e}'_{i,j,b} := \mathbf{e}_{i,j,b} + \mathbf{E}_{i,j,b}\mathbf{s}'$
$\mathsf{usk}[\mathsf{id}'] := \left([\mathbf{t}']_2, [\mathbf{u}']_2, [\mathbf{v}']_2\right)$
$\mathsf{udk}[\mathsf{id}'] := \left(\left[\mathbf{d}'_{i,j,b}\right]_2, \left[\mathbf{e}'_{i,j,b}\right]_2\right)_{\substack{p+2\le i\le L,\\ 1\le j\le i\alpha,\\ b\in\{0,1\}}}$
return $(\mathsf{usk}[\mathsf{id}'], \mathsf{udk}[\mathsf{id}'])$

Fig. 40. The scheme obtained by instantiating $\mathsf{HIBKEM}_{\mathsf{CPA}}[\mathsf{MAC}_1, \mathcal{U}_{2k,k}]$ with the SXDH assumption.

$\underline{\mathsf{Gen}(1^\lambda):}$
$\mathcal{PG} \xleftarrow{\$} \mathsf{PGGen}(1^\lambda)$
parse $\mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
$\mathbf{B} \xleftarrow{\$} \mathcal{U}_{3,1}$; $\mathbf{A} \xleftarrow{\$} \mathcal{U}_1$
for $i \in \{1, \dots, L\}$, $j \in \{1, \dots, i\alpha\}$, $b \in \{0,1\}$ **do**
  $\mathbf{X}_{i,j,b} \xleftarrow{\$} \mathbb{Z}_q^{1\times 3}$; $\mathbf{Y}_{i,j,b} \xleftarrow{\$} \mathbb{Z}_q^{1\times 3}$
  $\mathbf{Z}_{i,j,b} := \left(\mathbf{Y}_{i,j,b}^\top \mid \mathbf{X}_{i,j,b}^\top\right)\mathbf{A}$
  $\mathbf{D}_{i,j,b} := \mathbf{X}_{i,j,b} \cdot \mathbf{B}$; $\mathbf{E}_{i,j,b} := \mathbf{Y}_{i,j,b} \cdot \mathbf{B}$
$\mathbf{x}' \xleftarrow{\$} \mathbb{Z}_q$; $\mathbf{y}' \xleftarrow{\$} \mathbb{Z}_q$; $\mathbf{z}' := (\mathbf{y}' \mid \mathbf{x}') \cdot \mathbf{A}$
$\widetilde{\mathbf{Z}} := \left(\left[\mathbf{Z}_{i,j,b}\right]_1\right)_{1\le i\le L, 1\le j\le i\alpha, b\in\{0,1\}}$
$\mathsf{pk} := \left(\mathcal{PG}, [\mathbf{A}]_1, \widetilde{\mathbf{Z}}, [\mathbf{z}']_1\right)$
$\widetilde{\mathsf{dk}} := \left(\left[\mathbf{D}_{i,j,b}\right]_2, \left[\mathbf{E}_{i,j,b}\right]_2\right)_{\substack{1\le i\le L, b\in\{0,1\},\\ 1\le j\le i\alpha}}$
$\mathsf{dk} := \left([\mathbf{B}]_2, \widetilde{\mathsf{dk}}\right)$
$\mathsf{sk} := \left(\mathsf{sk}_{\mathsf{MAC}}, \left(\mathbf{Y}_{i,j,b}\right)_{\substack{1\le i\le L, b\in\{0,1\},,\\ 1\le j\le i\alpha}}, \mathbf{y}'\right)$
return $(\mathsf{pk}, \mathsf{dk}, \mathsf{sk})$

$\underline{\mathsf{Ext}(\mathsf{sk}, \mathsf{id} \in \mathcal{S}^p):}$
for $i \in \{1, \dots, p\}$ **do** $\mathbf{s}_i \xleftarrow{\$} \mathbb{Z}_q$; $\mathbf{t}_i := \mathbf{B}\mathbf{s}_i$
$\mathbf{u} := \sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{X}_{i,j,[\![\mathsf{m}]\!]_j}\mathbf{t}_i + \mathbf{x}'$
$\mathbf{v} := \sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{Y}_{i,j,[\![\mathsf{id}]\!]_j}\mathbf{t}_i + \mathbf{y}'$
return $\left(\left([\mathbf{t}_i]_2\right)_{1\le i\le p}, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$

$\underline{\mathsf{Del}(\mathsf{dk}, \mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}], \mathsf{id} \in \mathcal{S}^p, \mathsf{id}_{p+1}):}$
parse $\mathsf{usk}[\mathsf{id}] =: \left(\left([\mathbf{t}_i]_2\right)_{1\le i\le p}, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$
for $i \in \{1, \dots, p\}$ **do**
  $\mathbf{s}_i' \xleftarrow{\$} \mathbb{Z}_q$; $\mathbf{t}_i' := \mathbf{t}_i + \mathbf{B}\mathbf{s}_i'$
$\mathbf{s}_{p+1}' \xleftarrow{\$} \mathbb{Z}_q$; $\mathbf{t}_{p+1}' := \mathbf{B}\mathbf{s}_{p+1}'$
$\mathsf{id}' := (\mathsf{id}_1, \dots, \mathsf{id}_p, \mathsf{id}_{p+1})$
$\mathbf{u}' := \mathbf{u} + \sum_{i=1}^{p+1}\sum_{j=1}^{i\alpha} \mathbf{D}_{i,j,[\![\mathsf{id}']\!]_j}\mathbf{s}_i'$
$\mathbf{v}' := \mathbf{v} + \sum_{i=1}^{p+1}\sum_{j=1}^{i\alpha} \mathbf{E}_{i,j,[\![\mathsf{id}']\!]_j}\mathbf{s}_i'$
return $\left(\left([\mathbf{t}']_2\right)_{1\le i\le p+1}, [\mathbf{u}']_2, [\mathbf{v}']_2\right)$

$\underline{\mathsf{Enc}(\mathsf{pk}, \mathsf{id} \in \mathcal{S}^p):}$
$\mathbf{r} \xleftarrow{\$} \mathbb{Z}_q$; $\mathbf{c}_0 := \mathbf{A}\mathbf{r}$
for $i \in \{1, \dots, p\}$ **do**
  $\mathbf{c}_{1,i} := \sum_{j=1}^{i\alpha} \mathbf{Z}_{i,j,[\![\mathsf{id}]\!]_j}^\top \mathbf{r}$
$\mathsf{C} := \left([\mathbf{c}_0]_1, \left([\mathbf{c}_{1,i}]_1\right)_{1\le i\le p}\right)$
$\mathsf{K} := \mathbf{z}' \cdot \mathbf{r}$
return $\left([\mathsf{K}]_T, \mathsf{C}\right)$

$\underline{\mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id} \in \mathcal{S}^p, \mathsf{C}):}$
parse $\mathsf{usk}[\mathsf{id}] =: \left(\left([\mathbf{t}_i]_2\right)_{1\le i\le p}, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$
parse $\mathsf{C} =: \left([\mathbf{c}_0]_1, \left([\mathbf{c}_{1,i}]_1\right)_{1\le i\le p}\right)$
$[\mathsf{K}]_T := \left[\mathbf{c}_0^\top\right]_1 \circ \begin{bmatrix}\mathbf{v}\\ \mathbf{u}\end{bmatrix}_2 - \sum_{i=1}^{p}\left(\left[\mathbf{c}_{1,i}^\top\right]_1 \circ [\mathbf{t}_i]_2\right)$
return $[\mathsf{K}]_T$

Fig. 41. The scheme obtained by instantiating $\mathsf{HIBKEM}_{\mathsf{CPA}}[\mathsf{MAC}_2, \mathcal{U}_{2k,k}]$ with the SXDH assumption.

$\underline{\mathsf{Gen}(1^\lambda):}$
$\mathcal{PG} \xleftarrow{\$} \mathsf{PGGen}(1^\lambda)$
parse $\mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
$\mathbf{B} \xleftarrow{\$} \mathcal{U}_{3,1};\ \mathbf{A} \xleftarrow{\$} \mathcal{U}_1$
for $i \in \{1, \dots, L\},\ j \in \{1, \dots, i\alpha\},\ b \in \{0,1\}$ **do**
  $\mathbf{X}_{i,j,b} \xleftarrow{\$} \mathbb{Z}_q^{1\times 3};\ \mathbf{Y}_{i,j,b} \xleftarrow{\$} \mathbb{Z}_q^{1\times 3}$
  $\mathbf{Z}_{i,j,b} := \left(\mathbf{Y}_{i,j,b}^\top \mid \mathbf{X}_{i,j,b}^\top\right)\mathbf{A}$
$\mathbf{x}' \xleftarrow{\$} \mathbb{Z}_q;\ \mathbf{y}' \xleftarrow{\$} \mathbb{Z}_q;\ \mathbf{z}' := (\mathbf{y}' \mid \mathbf{x}') \cdot \mathbf{A}$
$\widetilde{\mathbf{Z}} := \left(\left[\mathbf{Z}_{i,j,b}\right]_1\right)_{1\le i\le L, 1\le j\le i\alpha, b\in\{0,1\}}$
$\mathsf{pk} := \left(\mathcal{PG}, [\mathbf{A}]_1, \widetilde{\mathbf{Z}}, [\mathbf{z}']_1\right)$
$\mathsf{sk} := \left(\mathsf{sk}_{\mathsf{MAC}}, \left(\mathbf{Y}_{i,j,b}\right)_{\substack{1\le i\le L, b\in\{0,1\},\\ 1\le j\le i\alpha}}, \mathbf{y}'\right)$
return $(\mathsf{pk}, \mathsf{sk})$

$\underline{\mathsf{Ext}(\mathsf{sk}, \mathsf{id} \in \mathcal{S}^p):}$
$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q;\ \mathbf{t} := \mathbf{B}\mathbf{s}$
$\mathbf{S} \xleftarrow{\$} \mathbb{Z}_q \setminus \{0\};\ \mathbf{T} := \mathbf{B} \cdot \mathbf{S}$
$\mathbf{u} := \sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{X}_{i,j,[\![\mathsf{id}]\!]_j}\mathbf{t} + \mathbf{x}'$
$\mathbf{U} := \sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{X}_{i,j,[\![\mathsf{id}]\!]_j}\mathbf{T}$
$\mathbf{v} := \sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{Y}_{i,j,[\![\mathsf{id}]\!]_j}\mathbf{t} + \mathbf{y}'$
$\mathbf{V} := \sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{Y}_{i,j,[\![\mathsf{id}]\!]_j}\mathbf{T}$
for $i \in \{p+1, \dots, L\},\ j \in \{1, \dots, i\alpha\},\ b \in \{0,1\}$ **do**
  $\mathbf{d}_{i,j,b} := \mathbf{X}_{i,j,b}\mathbf{t};\ \mathbf{D}_{i,j,b} := \mathbf{X}_{i,j,b}\mathbf{T}$
  $\mathbf{e}_{i,j,b} := \mathbf{Y}_{i,j,b}\mathbf{t};\ \mathbf{E}_{i,j,b} := \mathbf{Y}_{i,j,b}\mathbf{T}$
$\mathsf{usk}[\mathsf{id}] := \left([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$
$\mathsf{udk}_1[\mathsf{id}] := \left([\mathbf{T}]_2, [\mathbf{U}]_2, [\mathbf{V}]_2\right)$
$\mathsf{udk}_2[\mathsf{id}] := \Big(\left[\mathbf{d}_{i,j,b}\right]_2, \left[\mathbf{D}_{i,j,b}\right]_2, \left[\mathbf{e}_{i,j,b}\right]_2, \left[\mathbf{E}_{i,j,b}\right]_2\Big)_{p+1\le i\le L, 1\le j\le i\alpha}$
return $(\mathsf{usk}[\mathsf{id}], (\mathsf{udk}_1[\mathsf{id}], \mathsf{udk}_2[\mathsf{id}]))$

$\underline{\mathsf{Del}(\mathsf{dk}, \mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}], \mathsf{id} \in \mathcal{S}^p, \mathsf{id}_{p+1}):}$
parse $\mathsf{usk}[\mathsf{id}] =: \left([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$
parse $\mathsf{udk}[\mathsf{id}] =: \left([\mathbf{T}]_2, [\mathbf{U}]_2, [\mathbf{V}]_2, \mathsf{udk}_2\right)$
parse $\mathsf{udk}_2 =: \Big(\left[\mathbf{d}_{i,j,b}\right]_2, \left[\mathbf{D}_{i,j,b}\right]_2, \left[\mathbf{e}_{i,j,b}\right]_2, \left[\mathbf{E}_{i,j,b}\right]_2\Big)_{p+1\le i\le L, 1\le j\le i\alpha}$
$\mathsf{id}' := (\mathsf{id}_1, \dots, \mathsf{id}_p, \mathsf{id}_{p+1})$
$\mathbf{u}' := \mathbf{u} + \sum_{j=1}^{(p+1)\alpha} \mathbf{d}_{p+1,j,[\![\mathsf{id}]\!]_j}$
$\mathbf{U}' := \mathbf{U} + \sum_{j=1}^{(p+1)\alpha} \mathbf{D}_{p+1,j,[\![\mathsf{id}]\!]_j}$
$\mathbf{v}' := \mathbf{v} + \sum_{j=1}^{(p+1)\alpha} \mathbf{e}_{p+1,j,[\![\mathsf{id}]\!]_j}$
$\mathbf{V}' := \mathbf{V} + \sum_{j=1}^{(p+1)\alpha} \mathbf{E}_{p+1,j,[\![\mathsf{id}]\!]_j}$
$\mathbf{s}' \xleftarrow{\$} \mathbb{Z}_q^1;\ \mathbf{t}' := \mathbf{t} + \mathbf{T} \cdot \mathbf{s}'$
$\mathbf{S}' \xleftarrow{\$} \mathbb{Z}_q \setminus \{0\};\ \mathbf{T}' := \mathbf{T}\mathbf{S}'$
$\mathbf{u}'' := \mathbf{u} + \mathbf{U}\mathbf{s}';\ \mathbf{v} := \mathbf{v} + \mathbf{V}\mathbf{s}'$
$\mathbf{U} := \mathbf{U} \cdot \mathbf{S}';\ \mathbf{V} := \mathbf{V} \cdot \mathbf{S}'$
for $i \in \{p+2, \dots, L\},\ j \in \{1, \dots, \ell'(i)\}$ **do**
  $\mathbf{d}'_{i,j,b} := \mathbf{d}_{i,j,b} + \mathbf{D}_{i,j,b}\mathbf{s}'$
  $\mathbf{e}'_{i,j,b} := \mathbf{e}_{i,j,b} + \mathbf{E}_{i,j,b}\mathbf{s}'$
  $\mathbf{D}'_{i,j,b} := \mathbf{D} \cdot \mathbf{S}';\ \mathbf{E}'_{i,j,b} := \mathbf{E} \cdot \mathbf{S}'$
$\mathsf{usk}[\mathsf{id}'] := \left([\mathbf{t}']_2, [\mathbf{u}'']_2, [\mathbf{v}'']_2\right)$
$\mathsf{udk}_1[\mathsf{id}'] := \left([\mathbf{T}']_2, [\mathbf{U}'']_2, [\mathbf{V}'']_2\right)$
$\mathsf{udk}_2[\mathsf{id}'] =: \Big(\left[\mathbf{d}'_{i,j,b}\right]_2, \left[\mathbf{D}'_{i,j,b}\right]_2, \left[\mathbf{e}'_{i,j,b}\right]_2, \left[\mathbf{E}'_{i,j,b}\right]_2\Big)_{p+1\le i\le L, 1\le j\le i\alpha}$
return $(\mathsf{usk}[\mathsf{id}'], \mathsf{udk}_1[\mathsf{id}'], \mathsf{udk}_2[\mathsf{id}'])$

$\underline{\mathsf{Enc}(\mathsf{pk}, \mathsf{id} \in \mathcal{S}^p):}$
$\mathbf{r} \xleftarrow{\$} \mathbb{Z}_q;\ \mathbf{c}_0 := \mathbf{A}\mathbf{r}$
$\mathbf{c}_1 := \sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{Z}_{i,j,[\![\mathsf{id}]\!]_j}\mathbf{r}$
$\mathsf{C} := \left([\mathbf{c}_0]_1, [\mathbf{c}_1]_1\right)$
$\mathsf{K} := \mathbf{z}' \cdot \mathbf{r}$
return $\left([\mathsf{K}]_T, \mathsf{C}\right)$

$\underline{\mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id} \in \mathcal{S}^p, \mathsf{C}):}$
parse $\mathsf{usk}[\mathsf{id}] =: \left([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{v}]_2\right)$
parse $\mathsf{C} =: \left([\mathbf{c}_0]_1, [\mathbf{c}_1]_1\right)$
$[\mathsf{K}]_T := e\left(\left[\mathbf{c}_0^\top\right]_1, \begin{bmatrix}\mathbf{v}\\ \mathbf{u}\end{bmatrix}_2\right) - e\left(\left[\mathbf{c}_1^\top\right]_1, [\mathbf{t}]_2\right)$
return $[\mathsf{K}]_T$

Fig. 42. The scheme obtained by instantiating $\mathsf{AHIBKEM}_{\mathsf{CPA}}[\mathsf{MAC}_1, \mathcal{U}_{2k,k}]$ with the SXDH assumption.