Tightly Secure Hierarchical Identity-Based Encryption

Roman Langrehr(✉) and Jiaxin Pan

Karlsruhe Institute of Technology, Karlsruhe, Germany
roman.langrehr@student.kit.edu, jiaxin.pan@kit.edu

Abstract. We construct the *first* tightly secure hierarchical identity-based encryption (HIBE) scheme based on standard assumptions, which solves an open problem from Blazy, Kiltz, and Pan (CRYPTO 2014). At the core of our constructions is a novel randomization technique that enables us to randomize user secret keys for identities with flexible length.

The security reductions of previous HIBEs lose at least a factor of Q, which is the number of user secret key queries. Different to that, the security loss of our schemes is only dependent on the security parameter. Our schemes are adaptively secure based on the Matrix Diffie-Hellman assumption, which is a generalization of standard Diffie-Hellman assumptions such as k-Linear. We have two tightly secure constructions, one with constant ciphertext size, and the other with tighter security at the cost of linear ciphertext size. Among other things, our schemes imply the *first* tightly secure identity-based signature scheme by a variant of the Naor transformation.

Keywords: Hierarchical identity-based encryption · Tight security · Affine message authentication codes

1 Introduction

1.1 Motivation

Tight security. Reductions are useful tools for proving the security of public-key cryptographic schemes. Asymptotically, a reduction shows that if there is an efficient adversary $\mathcal{A}$ that breaks the security of a scheme then we can have another adversary $\mathcal{R}$ that solves the underlying computationally hard problem. Concretely, a reduction provides a security bound for the scheme, $\varepsilon_{\mathcal{A}} \leq \ell \cdot \varepsilon_{\mathcal{R}}$,[1] where $\varepsilon_{\mathcal{A}}$ is the success probability of $\mathcal{A}$ and $\varepsilon_{\mathcal{R}}$ is that of $\mathcal{R}$. Ideally, it is more desirable to have ℓ as small as a constant. We say a reduction is *tight* if ℓ is a small constant and the running time of $\mathcal{A}$ is approximately the same as that of $\mathcal{R}$.

[1] Here we ignore the additive negligible terms for simplicity.

J. Pan—Supported by DFG grant HO 4534/4-1.

D. Lin and K. Sako (Eds.): PKC 2019, LNCS 11442, pp. 436–465, 2019.
https://doi.org/10.1007/978-3-030-17253-4_15

Most of the current works have considered the tightness notion called "almost tight security", where ℓ may linearly (or, even better, logarithmically) depend on the security parameter, but not on the size of $\mathcal{A}$.[2] Recently, tightly secure cryptographic schemes drew a large amount of attention (e.g. [1,3,8,11,12,16–18]), since tightly secure schemes do not need to compensate for any security loss.

(Hierarchical) identity-based encryption. The concept of identity-based encryption (IBE) was proposed by Shamir [31] to simplify the management of public keys and certificates. With an IBE scheme, one can encrypt a message under a recipient's identity id (for instance, email address or ID card number), and this encrypted message can be decrypted with user id's secret key from a trusted authority. The first constructions of IBE were given in 2001 [4,9,30] in the random oracle model.

A hierarchical IBE (HIBE) scheme [14,22] generalizes the concept of IBE and provides more functionality by forming levels of a hierarchy. In an L-level HIBE, a hierarchical identity is a vector of maximal L identities, and a user at level i can delegate a secret key for its descendants at level i' (where $i < i' \leq L$). Moreover, a user at level i is not supposed to decrypt any encryption from a recipient which is not amongst its descendants. HIBE schemes not only are more general than IBE schemes (for instance, an IBE is simply a 1-level HIBE), but also provide numerous applications. Most famous ones are CCA-secure IBEs [5] and identity-based signatures [24] from HIBE. Both implications are tight.

Adaptive security is a widely accepted security notion for (H)IBEs, where an adversary is allow to adaptively choose a challenge identity id^* after it sees the (master) public key and Q-many user secret keys for adversarial chosen identities. To achieve adaptive security in the standard model, the early IBE constructions require either non-tight reductions to the hardness of the underlying assumptions [7,23,27,33], or Q-type, non-static assumptions [13].

In 2013, Chen and Wee constructed the first tightly secure IBE based on static assumptions in the standard model [8]. After that, several works have been done to improve its efficiency and achieve stronger security [3,16,19,21]. However, constructing an L-level HIBE for $L > 1$ with a tight (i.e., independent of Q) security reduction to a standard assumption remains open.

HIBEs meet tightness: difficulties and the hope. Before analyzing the difficulties of achieving tightly secure HIBE, we consider the security loss of the current state-of-the-art HIBEs. The L-level HIBE from [33] has a relatively large security loss, Q^L, which depends on both Q and L. Although the security loss of more recent HIBEs [3,8,15,27,32] does not depends on the number of maximal levels L, they are still not tight and lose a factor of Q.

In general, it is harder to construct HIBEs than IBEs, since HIBEs allow public delegation of user secret keys, given the corresponding ancestor's secret key. Hence, given a tightly secure IBE, there is no (tight) black-box transformation to HIBE. The works of Lewko and Waters [28] show the potential difficulty

[2] In this paper, we do not distinguish almost tight security from tight security, but we will detail the security loss in the security proof and comparison of our schemes.

of constructing HIBE with tight reductions. More precisely, [28] proves that it is hard to have an HIBE scheme with security loss less than exponential in L, if the HIBE has rerandomizable user secret keys (over all "functional" user secret keys).

The first attempt of constructing tightly secure HIBEs is due to Blazy, Kiltz, and Pan (cf. the proceeding version and the first full version of [3]), where they tightly transform algebraic message authentication code (MAC) schemes to (H)IBE schemes. As long as the algebraic MAC has tight security, the resulting (H)IBE is tightly secure. The first version of their paper contains a tightly secure delegatable MAC, which results in a tightly secure HIBE. The resulting HIBE has bypassed the impossibility result of [28] and their user secret keys are only rerandomizable over all keys generated by the user secret key generation algorithm, which is only a subspace of all "functional" keys. However, shortly after its publication, a flaw was found in a proof step of the delegatable MAC, and they remove this tightly secure delegatable MAC from their paper. The flaw is basically due to the fact that the BKP randomization technique failed to randomize MAC tags (which is an important part of user secret keys) for hierarchical identities.

The hope of achieving tight security for HIBEs lies in developing a novel method that enables randomization of user secret keys for identities with flexible level.

1.2 Our Contributions

We answer the aforementioned open question affirmatively with two *tightly secure* hierarchical identity-based encryption schemes with identity space $\mathcal{ID} := (\{0,1\}^\alpha)^{\leq L}$: One with constant ciphertext size (in terms of the number of group elements) and $O(\alpha L^2)$ security loss, and the other with ciphertext size linear in L but $O(\alpha L)$ security loss. Both schemes are the *first* tightly secure HIBEs. We compare our schemes with the existing HIBE schemes in prime-order pairing groups in Table 1.

Furthermore, via the known tight transformations from [24] and [5], our HIBEs imply the *first* tightly secure identity-based signature and tightly CCA-secure HIBEs almost for free. We note that an $(L+1)$-level HIBE tightly implies an L-level CCA-secure HIBE via the CHK transformation [5] in the single-challenge setting.

Core idea. In a nutshell, the technical novelty of our constructions is a new randomization technique that enables us to randomize user secret keys with flexible identity length. This technique is motivated by the recent tightly CCA-secure public-key encryption of Gay et al. [11].

At the core of our constructions lie two new pseudorandom message authentication code (MAC) schemes for messages with flexible length. Their pseudorandomness can be proven with tight reductions to the Matrix Decisional Diffie-Hellman (MDDH) assumption [10]. The MDDH assumption is a generalization of the known standard Diffie-Hellman assumptions, such as the k-linear (k-LIN) assumption. Our MAC schemes have algebraic structures compatible with the

Table 1. Comparison of L-level HIBEs with identity-space $\mathcal{ID} = (\{0,1\}^\lambda)^{\leq L}$ in prime-order pairing groups. '$\lvert\mathsf{mpk}\rvert$', '$\lvert\mathsf{usk}\rvert$' and '$\lvert\mathsf{C}\rvert$' stand for the size of master public key, user secret key and ciphertext. 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 $\mathbb{G} := \mathbb{G}_1 = \mathbb{G}_2$. Q is the number of user secret key queries by the adversary.

Scheme	$\lvert\mathsf{mpk}\rvert$	$\lvert\mathsf{usk}\rvert$	$\lvert\mathsf{C}\rvert$	Loss	Assumption
Wat05 [33]	$O(\alpha L)\lvert\mathbb{G}_1\rvert$	$O(\alpha L)\lvert\mathbb{G}_2\rvert$	$(1+L)\lvert\mathbb{G}_1\rvert$	$O(\alpha Q)^L$	DBDH
Wat09 [32]	$O(L)\lvert\mathbb{G}_1\rvert$	$O(L)(\lvert\mathbb{G}_2\rvert + \lvert\mathbb{Z}_q\rvert)$	$O(L)(\lvert\mathbb{G}_1\rvert + \lvert\mathbb{Z}_q\rvert)$	$O(Q)$	2-LIN
Lew12 [27]	$60\lvert\mathbb{G}\rvert + 2\lvert\mathbb{G}_T\rvert$	$(60+10L)\lvert\mathbb{G}\rvert$	$10L$	$O(Q)$	2-LIN
CW13 [8]	$O(Lk^2)(\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_2\rvert)$	$O(Lk)\lvert\mathbb{G}_2\rvert$	$(2k+2)\lvert\mathbb{G}_1\rvert$	$O(Q)$	k-LIN
BKP14 [3]	$O(Lk^2)(\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_2\rvert)$	$O(Lk)\lvert\mathbb{G}_2\rvert$	$(2k+2)\lvert\mathbb{G}_1\rvert$	$O(Q)$	k-LIN
GCTC16 [15]	$18\lvert\mathbb{G}_1\rvert + 3\lvert\mathbb{G}_T\rvert$	$(18\lceil L/3\rceil + 18 - 3L)\lvert\mathbb{G}_2\rvert$	$9\lceil L/3\rceil\lvert\mathbb{G}_1\rvert$	$O(Q)$	SXDH
Ours (Fig. 11)	$O(\alpha L^2)(\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_2\rvert)$	$O(\alpha L^2)\lvert\mathbb{G}_2\rvert$	$5\lvert\mathbb{G}_1\rvert$	$O(\alpha L^2)$	SXDH
Ours (Fig. 12)	$O(\alpha L^2)(\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_2\rvert)$	$O(L)\lvert\mathbb{G}_2\rvert$	$(3L+2)\lvert\mathbb{G}_1\rvert$	$O(\alpha L)$	SXDH

BKP transformation. In the end, together with a variant of the BKP framework [3], we can tightly randomize user secret keys with hierarchical identities and we have tightly secure HIBEs.

A CLOSER LOOK AT THE BKP FRAMEWORK. The BKP framework proposes the notion of affine MACs and transforms it to an (H)IBE scheme with pairings. Their transformation is tightness-preserving. Under the MDDH assumption, if the affine MAC is tightly secure, then the (H)IBE is also tightly secure. It is worth mentioning that the BKP transformation and its variants are widely used in constructing identity-based encryption [19] with multi-challenge CCA security, predicate encryption [6,34], quasi-adaptive NIZK [26], and structure-preserving signature [12,25] based on standard, static assumptions.

We recall their tightly secure MAC, $\mathsf{MAC}_{\mathsf{NR}}$, based on the Naor-Reingold pseudorandom function [29], which is implicitly in the Chen-Wee (CW) IBE [8] as well. $\mathsf{MAC}_{\mathsf{NR}}$ is defined over an additive prime-order group $\mathbb{G}_2 := \langle P_2 \rangle$ and its message space is corresponding to the identity space of the resulting IBE. We use the implicit notation $[x]_2 := xP_2$ from [10]. $\mathsf{MAC}_{\mathsf{NR}}$ chooses $\mathbf{B} \in \mathbb{Z}_q^{(k+1)\times k}$ according to the underlying assumption. For message space $\mathcal{M} := \{0,1\}^\alpha$, its secret key is defined as

$$\mathsf{sk}_{\mathsf{MAC}} := \left((\mathbf{x}_{i,b})_{1\leq i\leq \alpha, b=0,1}, x_0' \right) \in \left(\mathbb{Z}_q^{k\cdot 2} \right)^\alpha \times \mathbb{Z}_q$$

and its MAC tag contains a message-independent vector $[\mathbf{t}]_2$ and a message-dependent value $[u]_2$ in the form of

$$\begin{aligned} \mathbf{t} &= \overline{\mathbf{B}}\mathbf{s} \in \mathbb{Z}_q^k \quad \text{for} \quad \mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k \\ u &= \sum\nolimits_i \mathbf{x}_{i,\mathsf{m}_i}^\top \mathbf{t} + x_0' \in \mathbb{Z}_q \end{aligned}, \tag{1}$$

where $\overline{\mathbf{B}}$ denotes the first k rows of $\mathbf{B}$. The BKP transformation requires the MAC scheme has psedorandomness against chosen-message attacks (PR-CMA security), which is a decisional variant of the standard existential unforgeability against chosen-message attacks ($\mathsf{EUF\text{-}CMA}$ security). In order to provide a simpler and more intuitive discussion, we consider the standard $\mathsf{EUF\text{-}CMA}$ security of $\mathsf{MAC_{NR}}$, where an adversary $\mathcal{A}$ is allowed to see many MAC tags $\tau_{\mathsf{m}} := ([\mathbf{t}_{\mathsf{m}}]_2, [u_{\mathsf{m}}]_2)$ on messages m of its choice and tries to forge a fresh and valid forgery (m^*, τ^*) which satisfies Eq. (1).

Following the CW argument [8], by a hybrid argument on the bit length of m, one can show that the value $[u]_2$ is pseudorandom such that it is hard for an adversary to forge. By embedding the problem challenge in $\mathbf{t}$ and $\mathbf{x}_{i+1,1-b}$, the CW argument can manage to develop the following random function RF_{i+1} for $(i+1)$-bit messages from a random function RF_i for i-bit messages on-the-fly:

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

where b is the guess for the $(i+1)$-th bit of m^* and $\mathsf{m}_{|i}$ is the first i bits of m. Such an argument works well if messages have fixed length. For messages m with fixed length, an adversary can see the output of either RF_i (in Hybrid i) or RF_{i+1} (in Hybrid $i+1$), but not both. However, that is not the case for messages m' with flexible length.

Concretely, identities for HIBEs are messages with flexible level. If we follow the CW and BKP arguments, we first need to develop a random function at the 2-level based on that at the 1-level. The critical case happens when we switch from Hybrid α (the end of randomization at the 1-level) to Hybrid $\alpha+1$ (the beginning of randomization at the 2-level). If we define $\mathsf{RF}_{\alpha+1}$ (with message space $\{0,1\}^{\alpha} \cup \{0,1\}^{\alpha+1}$) via Eq. (2) based on random functions $\mathsf{RF}_{\alpha}, \mathsf{RF}'_{\alpha}$ (with message space $\{0,1\}^{\alpha}$), then we have $\mathsf{RF}_{\alpha+1}(\mathsf{m}) = \mathsf{RF}_{\alpha+1}(\mathsf{m}||b)$ for a $\mathsf{m} \in \{0,1\}^{\alpha}$ and that means the resulting $\mathsf{RF}_{\alpha+1}$ is not a random function for messages with flexible level.

1.3 Our Approach: Independent Randomization

To circumvent the aforementioned problem, we propose a suitable pseudorandom MAC, which isolates the tag randomization for messages with different levels. Our strategy is to randomize tags for messages with only one level first, and then for those with two levels, and so on. By a novel use of the recent subspace randomization refined from [11], tags for messages with different levels are randomized independently.

Affine MACs with levels. We consider a new notion of affine MACs, called *affine MACs with levels*, and we give two constructions of it. This new notion considers messages with flexible levels and enable us to develop independent random functions RF_{α} for messages with only one level (i.e., in $\{0,1\}^{\alpha}$), and $\mathsf{RF}'_{2\cdot\alpha}$ for messages with only two levels (i.e., in $\{0,1\}^{2\alpha}$), and so on. For simplicity, we present an overview of our technique in terms of 2-level HIBEs ($L=2$), namely, the hierarchical identity space $\mathcal{ID} := (\{0,1\}^{\alpha})^{\leq 2}$. We denote 1-level messages as $\mathsf{m} \in \{0,1\}^{\alpha}$ and 2-level messages as $\mathsf{m}' \in \{0,1\}^{\alpha\cdot 2}$.

Our first MAC construction MAC_1's secret keys have the form of

$$\mathsf{sk}_{\mathsf{MAC}_1} := \Big((\mathbf{x}_{i,b})_{i,b} , \boxed{(\hat{\mathbf{x}}_{j,b})_{1\le j\le 2\alpha,b}} , x_0' \Big) \in \left(\mathbb{Z}_q^{k\cdot 2}\right)^{\alpha} \times \boxed{\left(\mathbb{Z}_q^{k\cdot 2}\right)^{\alpha\cdot 2}} \times \mathbb{Z}_q.$$

Value u in the MAC tags for $\mathsf{m} \in \{0,1\}^{\alpha}$ and $\mathsf{m}' \in \{0,1\}^{2\alpha}$ has the form of

$$\begin{aligned} u_{\mathsf{m}} &:= \sum_{i=1}^{\alpha} \mathbf{x}_{i,\mathsf{m}_i}^{\top}\mathbf{t} + x_0' \in \mathbb{Z}_q \\ u_{\mathsf{m}'} &:= \sum_{i=1}^{\alpha} \mathbf{x}_{i,\mathsf{m}_i'}^{\top}\mathbf{t} + \boxed{\sum_{j=1}^{2\alpha} \hat{\mathbf{x}}_{j,\mathsf{m}_j'}^{\top}\mathbf{t}} + x_0' \in \mathbb{Z}_q \end{aligned}. \tag{3}$$

By a similar argument as in the BKP we can randomize all the u_{m} for 1-level messages m and, after the first level messages randomization, u_{m} has the form

$$u_{\mathsf{m}} := \sum_{i=1}^{\alpha} \mathbf{x}_{i,\mathsf{m}_i}^{\top}\mathbf{t} + \mathsf{RF}_{\alpha}(\mathsf{m}),$$

namely, we replace x_0' with $\mathsf{RF}_{\alpha}(\mathsf{m})$, but this affects the $u_{\mathsf{m}'}$ for 2-level messages m' as well. More precisely, $u_{\mathsf{m}'}$ carries the random function RF_{α} and has the form

$$u_{\mathsf{m}'} := \left(\sum_{i=1}^{\alpha} \mathbf{x}_{i,\mathsf{m}_i'}^{\top} + \sum_{j=1}^{2\alpha} \hat{\mathbf{x}}_{j,\mathsf{m}_j'}^{\top} \right) \mathbf{t} + \mathsf{RF}_{\alpha}(\mathsf{m}'_{|\alpha}).$$

If we continue to randomize $u_{\mathsf{m}'}$, we will run into the exact same problem as in the CW or BKP randomization.

Motivated by [11], we hide RF_{α} in some orthogonal space. By switching $\mathbf{t}$ into the "right" span, RF_{α} appears in u_{m}, but gets canceled in $u_{\mathsf{m}'}$. Concretely, we choose $\mathbf{B} \xleftarrow{\$} \mathbb{Z}_q^{3k\times k}$ and $\mathbf{B}^{\perp} \in \mathbb{Z}_q^{3k\times 2k}$ is a kernel matrix of $\mathbf{B}$ such that $(\mathbf{B}^{\perp})^{\top}\mathbf{B} = \mathbf{0}$. We replace $\mathbf{t} \xleftarrow{\$} \mathbb{Z}_q^{k}$ with larger $\mathbf{t} \xleftarrow{\$} \mathbb{Z}_q^{3k}$. We embed the random function RF_{α} into the kernel of $\mathbf{B}$ and u_{y} ($\mathsf{y} \in \{\mathsf{m}, \mathsf{m}'\}$) has the form

$$u_{\mathsf{y}} := \big(\quad \sim \quad + \quad \mathsf{RF}_{\alpha}(\mathsf{y}_{|\alpha})(\mathbf{B}^{\perp})^{\top} \big)\, \mathbf{t} + x_0'$$

where "$\sim$" denotes corresponding summation terms. During the randomization for 1-level messages, if we choose $\mathbf{t} \in \mathsf{Span}(\mathbf{B}) := \{\mathbf{v} \mid \exists \mathbf{s} \in \mathbb{Z}_q^{k} : \mathbf{v} = \mathbf{B}\mathbf{s}\}$ for 2-level messages m', then RF_{α} will get canceled out; and if we choose $\mathbf{t} \notin \mathsf{Span}(\mathbf{B})$ for 1-level messages m, then RF_{α} will appear and u_{m} gets randomized. After the randomization for 1-level messages, $u_{\mathsf{m}'}$ for 2-level messages m' is distributed the same as in Eq. (3) so that we can start 2-level randomization from a constant random function $\mathsf{RF}_0'(\epsilon)$ multiplying with $(\mathbf{B}^{\perp})^{\top}$, where ϵ denotes the empty string.

The way of developing RF_{α} (or $\mathsf{RF}_{2\cdot\alpha}'$, respectively) from RF_0 (or RF_0', respectively) is similar to [11]. Roughly, 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 the span of $\mathbf{B}, \mathbf{B}_0, \mathbf{B}_1$. The span of

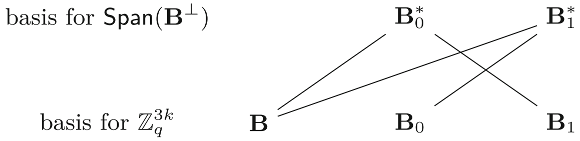
basis for $\mathsf{Span}(\mathbf{B}^\perp)$
$\mathbf{B}_0^*$
$\mathbf{B}_1^*$
basis for $\mathbb{Z}_q^{3k}$
$\mathbf{B}$
$\mathbf{B}_0$
$\mathbf{B}_1$

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

$\mathbf{B}^\perp$ 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 Fig. 1. After the decomposition of linear spaces, $\mathsf{RF}_i(\mathsf{m}_{|i})(\mathbf{B}^\perp)^\top = \mathsf{RF}_i^{(0)}(\mathsf{m}_{|i})(\mathbf{B}_0^*)^\top + \mathsf{RF}_i^{(1)}(\mathsf{m}_{|i})(\mathbf{B}_1^*)^\top$. By using the MDDH assumption, we can switch $[\mathbf{t}]_2$ to the right span and develop $\mathsf{RF}_{i+1}(\mathsf{m}_{|i+1})(\mathbf{B}^\perp)^\top$ from $\mathsf{RF}_i(\mathsf{m}_{|i})(\mathbf{B}^\perp)^\top$ in a tight fashion.

In order to have public delegation, the user secret keys at level 1 contain delegation terms $[\hat{\mathbf{x}}_{j,b}^\top \mathbf{t}]_2$. Since our randomization at different levels are isolated, the published terms will not affect our randomization strategy. Details are given in Sect. 3.1. In the end, our security reduction loses a factor of $O(\alpha L^2)$ due to L-many randomization loops and the fact that in each loop a additional factor of $O(\alpha L)$ is required. Applying a variant of the BKP transformation (cf. Sect. 4), we obtain the *first* HIBE scheme with tight security.

Achieving tighter security. Our second MAC construction (MAC_2 in Sect. 3.2) parallelizes the above randomization strategy and it has a scheme with security loss $O(\alpha L)$. The cost of doing this is to have different $\mathbf{t}_i$ at different level for a message with L levels, which results in an HIBE with $O(L)$-size ciphertext via the BKP transformation.

1.4 More Related Work and Open Problems

Bader et al. [2] use some idea from the BKP HIBE to construct digital signature schemes with corruptions, but it does not involve any randomization for messages with flexible length, and thus it does not have the same issue as the BKP.

Very recently, Hofheinz, Jia, and Pan [19] extend the BKP construction with the information-theoretical Cramer-Shoup-like argument of [11] to answer multiple challenge ciphertext queries for IBE. However, we do not know whether their technique and a similar one from [16] can work directly here to construct tightly multi-challenge secure HIBE. We leave achieving tight multi-challenge security for HIBEs as an open problem. Another interesting direction is to improve the efficiency of our schemes.

2 Preliminaries

Notations. We use $x \overset{\$}{\leftarrow} \mathcal{S}$ to denote the process of sampling an element x from $\mathcal{S}$ uniformly at random if $\mathcal{S}$ is a set. For positive integers $k > 1, \eta \in \mathbb{Z}^+$ 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 $\underline{\mathbf{v}} \in \mathbb{Z}_q^\eta$. For a string $\mathsf{m} \in \Sigma^n$, m_i denotes the i-th component of m $(1 \leq i \leq n)$ 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 $\mathsf{m}_1 || \dots || \mathsf{m}_p$. Thus for $1 \leq i \leq np$ $[\![\mathsf{m}]\!]_i$ denotes the i-th bit of $\mathsf{m}_1 || \dots || \mathsf{m}_p$ and $[\![\mathsf{m}]\!]_{|i}$ denotes the i-bit-long prefix of $\mathsf{m}_1 || \dots || \mathsf{m}_p$.

All our algorithms are probabilistic polynomial time unless we stated otherwise. If $\mathcal{A}$ is an algorithm, then we write $a \overset{\$}{\leftarrow} \mathcal{A}(b)$ to denote the random variable that outputted by $\mathcal{A}$ on input b.

Games. Following [3], we use code-based games to define and prove security. A game G contains procedures Init and Finalize, and some additional procedures $\mathrm{P}_1, \dots, \mathrm{P}_n$, 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.

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, P_1 and P_2 are generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively, and $e : \mathbb{G}_1 \times \mathbb{G}_2$ 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 our constructions 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 implicit representation of group elements as in [10]. 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 $\mathbb{G}_s$. $\mathsf{Span}(\mathbf{A}) := \{\mathbf{Ar} | \mathbf{r} \in \mathbb{Z}_q^m\} \subset \mathbb{Z}_q^n$ denotes the linear span of $\mathbf{A}$, and similarly $\mathsf{Span}([\mathbf{A}]_s) := \{[\mathbf{Ar}]_s | \mathbf{r} \in \mathbb{Z}_q^m\} \subset \mathbb{G}_s^n$. 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 [10].

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* GGen *in group $\mathbb{G}_s$ if for all PPT adversaries $\mathcal{A}$, it holds that*

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

is negligible where the probability is taken over $\mathcal{G} \xleftarrow{\$} \mathsf{GGen}(1^\lambda)$, $\mathbf{A} \xleftarrow{\$} \mathcal{D}_{\ell,k}, \mathbf{w} \xleftarrow{\$} \mathbb{Z}_q^k$ 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 [11] 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 [11]). *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. Precisely, for each adversary $\mathcal{A}$ there exists an adversary $\mathcal{B}$ and vice versa with*

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

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

Lemma 2 ($\mathcal{D}_{\ell,k}$-MDDH $\Rightarrow$ $\mathcal{U}_k$-MDDH [10]). *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. Precisely, for each adversary $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

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

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 $([\mathbf{A}], [\mathbf{AW}])$ and $([\mathbf{A}], [\mathbf{U}])$. 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. For the uniform distribution $\mathcal{U}_{\ell,k}$, the security loss $\ell - k$ can be avoided by applying Lemma 3 to the $\mathcal{U}_k$ distribution and then use Lemma 1 on each of the $\mathcal{U}_k$ instances to get a $\mathcal{U}_{\ell,k}$ instance.

Lemma 3 (Random self-reducibility [10]). *For $\ell > k$ and any matrix distribution $\mathcal{D}_{\ell,k}$, $\mathcal{D}_{\ell,k}$-MDDH is random self-reducible. In particular, for any $Q \geq 1$ and any adversary $\mathcal{A}$ there exists a adversary $\mathcal{B}$ with*

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

where $\mathcal{G} \overset{\$}{\leftarrow} \mathsf{GGen}\left(1^{\lambda}\right)$, $\mathbf{A} \overset{\$}{\leftarrow} \mathcal{D}_{\ell,k}$, $\mathbf{W} \overset{\$}{\leftarrow} \mathbb{Z}_q^{k \times Q}$, $\mathbf{U} \overset{\$}{\leftarrow} \mathbb{Z}_q^{(k+1) \times Q}$, and $T\left(\mathcal{A}\right) \approx T\left(\mathcal{B}\right) + Q \cdot \mathsf{poly}\left(\lambda\right)$.

2.2 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 [20] 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 4 (Hierarchical identity-based key encapsulation mechanism). *A hierarchical identity-based key encapsulation mechanism (HIBE)* HIBKEM *consists of three PPT algorithms* $\mathsf{HIBKEM} = (\mathsf{Gen}, \mathsf{Del}, \mathsf{Ext}, \mathsf{Enc}, \mathsf{Dec})$ *with the following properties.*

- *The probabilistic key generation algorithm* $\mathsf{Gen}(\mathsf{par})$ *returns the (master) public/secret key and delegation key* $(\mathsf{pk}, \mathsf{sk}, \mathsf{dk})$. *Note that for some of our constructions* dk *is empty. We assume that* pk *implicitly defines a hierarchical identity space $\mathcal{ID} = \mathcal{S}^{\leq L}$, for some base identity set $\mathcal{S}$, and a key space $\mathcal{K}$, and 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 value* $\mathsf{udk}[\mathsf{id}]$ *for hierarchical identity* $\mathsf{id} \in \mathcal{ID}$.
- *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* $1 \leq |\mathsf{id}| \leq m - 1$.
- *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* $\perp$.

For correctness we require that 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* $\mathsf{Enc}(\mathsf{pk}, \mathsf{id})$*:*

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

Moreover, we also require the distribution of $\mathsf{usk}[\mathsf{id}|\mathsf{id}_{p+1}]$ *from* $\mathsf{Del}(\mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}], \mathsf{id}, \mathsf{id}_{p+1})$ *is identical to the one from* $\mathsf{Ext}(\mathsf{sk}, \mathsf{id}|\mathsf{id}_{p+1})$*.*

In our HIBKEM definition we make the delegation key dk explicit to make our constructions 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 Fig. 2.

```
Init:
    $(\mathsf{pk}, \mathsf{sk}, \mathsf{dk}) \xleftarrow{\$} \mathsf{Gen}(\lambda)$
    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(id*):                                   //one query
    $(\mathsf{K}^*, \mathsf{C}^*) \xleftarrow{\$} \mathsf{Enc}(\mathsf{pk}, \mathsf{id}^*)$
    $\boxed{\mathsf{K}^* \xleftarrow{\$} \mathcal{K}}$
    Return $(\mathsf{K}^*, \mathsf{C}^*)$

Finalize($\beta \in \{0, 1\}$):
    Return $(\mathsf{Prefix}(\mathsf{id}^*) \cap \mathcal{Q}_{\mathcal{ID}} = \emptyset) \wedge \beta$
```

Fig. 2. Games $\mathsf{IND\text{-}HID\text{-}CPA}_{\mathsf{real}}$ and $\boxed{\mathsf{IND\text{-}HID\text{-}CPA}_{\mathsf{rand}}}$ for defining IND-HID-CPA-security. For any identity $\mathsf{id} \in \mathcal{S}^p$, $\mathsf{Prefix}(\mathsf{id})$ denotes the set of all prefixes of id.

Definition 5 (IND-HID-CPA Security). *A hierarchical identity-based key encapsulation scheme* HIBKEM *is* IND-HID-CPA*-secure if for all PPT* $\mathcal{A}$*,*

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

is negligible.

3 Affine MAC with Levels

The core of our HIBE constructions is a Message Authentication Code with suitable algebraic structures and we call it affine MAC with levels. This is a generalization of the delegatable, affine MAC used in [3], namely, a delegatable, affine MAC is affine MAC with levels with $\ell(p) = 1$ for all $p \in \{1, \dots L\}$.

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* $\mathsf{sk}_{\mathsf{MAC}} := \left(\mathbf{B}, (\mathbf{x}_{l,i,j})_{1\le l\le \ell(L), 1\le i\le L, 1\le j\le \ell'(l,i)}, x'_0\right)$ *where* $\mathbf{B} \in \mathbb{Z}_q^{n\times n'}$, $\mathbf{x}_{l,i,j} \in \mathbb{Z}_q^n$ *for* $l \in \{1,\dots,\ell(L)\}$, $i \in \{1,\dots,L\}$, *and* $j \in \{0,\dots,\ell'(l,i)\}$ *and* $x'_0 \in \mathbb{Z}_q$.
- $\mathsf{Tag}\left(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m} \in \mathcal{S}^{p\le L}\right)$ *returns a tag* $\tau := \left(([\mathbf{t}_l]_2)_{1\le l\le \ell(p)}, [u]_2\right)$ *where*

$$\mathbf{t}_l := \mathbf{B}\mathbf{s}_l \quad \textit{for } \mathbf{s}_l \overset{\$}{\leftarrow} \mathbb{Z}_q^{n'} \quad (1 \le l \le \ell(p))$$

$$u := \sum_{l=1}^{\ell(p)} \left(\sum_{i=1}^{p} \sum_{j=1}^{\ell'(l,i)} f_{l,i,j}\left(\mathsf{m}_{|i}\right) \mathbf{x}_{l,i,j}^{\top} \right) \mathbf{t}_l + x'_0 \tag{4}$$

- $\mathsf{Ver}_{\mathsf{MAC}}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m}, \tau = ([\mathbf{t}]_2, [u]_2))$ *checks, whether Eq. (4) holds.*

The messages of MAC *have the form* $\mathsf{m} = (\mathsf{m}_1, \dots, \mathsf{m}_p)$ *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* $\ell : \{1,\dots,p\} \to \mathbb{N}_+$, $n, n' \in \mathbb{N}_+$ *and* $\ell' : \{1,\dots,p\} \times \{1,\dots,L\} \to \mathbb{N}_+$ *(*$1 \le i \le L$*) are arbitrary, scheme-depending parameters. The function* ℓ *must be monotonous increasing.*

Security Model. As security model for affine MACs with levels we use HPR_0-CMA-security as defined by the games in Fig. 3. This is a generalization of the HPR_0-CMA-security for delegatable, affine MACs defined in [3].

```
Init:
  $\mathsf{sk}_{\mathsf{MAC}} \overset{\$}{\leftarrow} \mathsf{Gen}_{\mathsf{MAC}}(\mathbb{G}_2, q, P_2)$
  Parse $\mathsf{sk}_{\mathsf{MAC}} =: (\mathbf{B}, \widetilde{\mathbf{x}}, x'_0)$
  Parse $\widetilde{\mathbf{x}} =: (\mathbf{x}_{l,i,j})_{1\le l\le \ell(L), 1\le i\le L, 1\le j\le \ell'(l,i)}$
  $\mathsf{dk} := \left(\left[\mathbf{x}_{l,i,j}^{\top}\mathbf{B}\right]_2\right)_{1\le l\le \ell(L), 1\le i\le L, 1\le j\le \ell'(l,i)}$
  return $\left([\mathbf{B}]_2, \mathsf{dk}\right)$

Eval($\mathsf{m} \in \mathcal{S}^p$):
  $\mathcal{Q}_{\mathcal{M}} = \mathcal{Q}_{\mathcal{M}} \cup \{\mathsf{m}\}$
  $\left([\mathbf{t}]_2, [u]_2\right) \overset{\$}{\leftarrow} \mathsf{Tag}(\mathsf{sk}, \mathsf{m})$
  for $l \in \{1,\dots,\ell(p)\}, i \in \{p+1,\dots,L\}, j \in \{1,\dots,\ell'(l,i)\}$ do $d_{l,i,j} = \mathbf{x}_{l,i,j}^{\top}\mathbf{t}_l$
  $\mathsf{tdk} := \left([d_{l,i,j}]_2\right)_{1\le l\le \ell(p), p+1\le i\le L, 1\le j\le \ell'(l,i)}$
  return $\left(([\mathbf{t}_l]_2)_{1\le l\le \ell(p)}, [u]_2, \mathsf{tdk}\right)$

Chal($\mathsf{m}^\star \in \mathcal{S}^p$):        // one query
  $h \overset{\$}{\leftarrow} \mathbb{Z}_q$
  for $l \in \{1,\dots,\ell(p)\}$ do
      $\mathbf{h}_{0,l} := \left(\sum_{i=1}^{L}\sum_{j=1}^{\ell'(l,i)} f_{l,i,j}\left(\mathsf{m}^\star_{|i}\right)\mathbf{x}_{l,i,j}\right) h$
  $h_1 = x'_0 \cdot h \in \mathbb{Z}_q$
  $\boxed{h_1 \overset{\$}{\leftarrow} \mathbb{Z}_q}$
  return $\left([h], ([\mathbf{h}_{0,l}]_1)_{1\le l\le \ell(p)}, [h_1]_T\right)$

Finalize($\beta \in \{0,1\}$):
  return $\beta \wedge (\mathsf{Prefix}(\mathsf{m}^\star) \cap \mathcal{Q}_{\mathcal{M}} = \emptyset)$
```

Fig. 3. Games HPR_0-$\mathsf{CMA}_{\mathsf{real}}$, and $\boxed{\mathsf{HPR}_0\text{-}\mathsf{CMA}_{\mathsf{rand}}}$ for defining HPR_0-CMA security for affine MACs with levels.

Definition 7 ($\mathsf{HPR_0\text{-}CMA}$ **Security).** *An affine MAC with levels is* $\mathsf{HPR_0\text{-}CMA}$ *secure in* $\mathbb{G}_2$ *if for all PPT adversaries* $\mathcal{A}$ *the function*

$$\mathsf{Adv}^{\mathsf{hpr_0\text{-}cma}}_{\mathsf{MAC},\mathbb{G}_2}(\mathcal{A}) := \left|\Pr\left[\mathsf{HPR_0\text{-}CMA}^{\mathcal{A}}_{\mathsf{real}} \Rightarrow 1\right] - \Pr\left[\mathsf{HPR_0\text{-}CMA}^{\mathcal{A}}_{\mathsf{rand}} \Rightarrow 1\right]\right|$$

is negligible.

3.1 Our First Construction

Let $(\mathbb{G}_2, q, P_2)$ be a group of prime order q. Our first affine MAC with levels $\mathsf{MAC}_1[\mathcal{U}_{3k,k}] := (\mathsf{Gen}_{\mathsf{MAC}}, \mathsf{Tag}, \mathsf{Ver}_{\mathsf{MAC}})$ with message space $\mathcal{ID} := \mathcal{S}^{\leq L} := (\{0,1\}^{\alpha})^{\leq L}$ is defined in Fig. 4. The identity vectors bit-length α and the maximum length L of the identity vectors can be chosen freely.[3] The resulting HIBE from this MAC has constant ciphertext length.

$\mathsf{MAC}_1[\mathcal{U}_{3k,k}]$ has $n := 3k$ and $n' := k$ where $k \in \mathbb{N}_+$ can be chosen arbitrary. To match the formal definition, $\mathbf{x}_{i,j,b}$ should be renamed to $\mathbf{x}_{i,2j-b}$ and $f_{i,2j-b}(\mathsf{m}_{|i}) := \left([\![\mathsf{m}_{|i}]\!]_j \overset{?}{=} b\right)$. Then we get $\ell(p) = 1$ and $\ell'(1,i) = 2i\alpha$.

```
$\underline{\mathsf{Gen}_{\mathsf{MAC}}(\mathbb{G}_2, q, P_2):}$
$\mathbf{B} \xleftarrow{\$} \mathcal{U}_{3k,k}$
for $i \in \{1,\ldots,L\}, j \in \{1,\ldots,i\alpha\}, b \in \{0,1\}$ do $\mathbf{x}_{i,j,b} \xleftarrow{\$} \mathbb{Z}_q^{3k}$
$x'_0 \xleftarrow{\$} \mathbb{Z}_q$
return $\mathsf{sk}_{\mathsf{MAC}} := \left(\mathbf{B}, (\mathbf{x}_{i,j,b})_{1\leq i\leq L, b\in\{0,1\}, 1\leq j\leq i\alpha}, x'_0\right)$

$\underline{\mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m} \in \mathcal{S}^p):}$
Parse $\mathsf{sk}_{\mathsf{MAC}} =: \left(\mathbf{B}, (\mathbf{x}_{i,j,b})_{1\leq i\leq L, b\in\{0,1\}, 1\leq j\leq i\alpha}, x'_0\right)$
$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{t} := \mathbf{B}\mathbf{s}$
$u := \left(\sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{x}^{\top}_{i,j,[\![\mathsf{m}]\!]_j}\right)\mathbf{t} + x'_0$
return $\tau := \left([\mathbf{t}]_2, [u]_2\right)$

$\underline{\mathsf{Ver}_{\mathsf{MAC}}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m} \in \mathcal{S}^p, \tau):}$
Parse $\mathsf{sk}_{\mathsf{MAC}} =: \left(\mathbf{B}, (\mathbf{x}_{i,j,b})_{1\leq i\leq L, b\in\{0,1\}, 1\leq j\leq i\alpha}, x'_0\right)$
Parse $\mathsf{m} =: (\mathsf{m}_1, \ldots, \mathsf{m}_p)$
Parse $\tau =: \left([\mathbf{t}]_2, [u]_2\right)$
return $u \overset{?}{=} \left(\sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{x}^{\top}_{i,j,[\![\mathsf{m}]\!]_j}\right)\mathbf{t} + x'_0$
```

Fig. 4. Our first affine MAC

[3] A different bitlength on each level is possible as well, but we assume it is α on each level to ease notation.

Theorem 1 (Security of $\mathsf{MAC}_1[\mathcal{U}_{3k,k}]$). $\mathsf{MAC}_1[\mathcal{U}_{3k,k}]$ *is tightly* HPR_0-CMA *secure in* $\mathbb{G}_2$ *under the* $\mathcal{U}_k$-MDDH *assumption for* $\mathbb{G}_2$*. Precisely, for all adversaries* $\mathcal{A}$ *there exists an adversary* $\mathcal{B}$ *with*

$$\mathsf{Adv}^{\mathsf{hpr}_0\text{-}\mathsf{cma}}_{\mathsf{MAC}_1[\mathcal{U}_{3k,k}],\mathbb{G}_2}(\mathcal{A}) \leq \left(4(\alpha+1)L + 4\alpha L^2\right)\left(\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{GGen},\mathbb{G}_2}(\mathcal{B}) + \frac{1}{q-1}\right) + \frac{LQ}{q^{2k}}$$

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

Proof. The proof uses a hybrid argument with the hybrids G_0 (the HPR_0-$\mathsf{CMA}_{\mathsf{real}}$ game), G_1, $\mathsf{G}_{2,\hat{\imath},0}$, $\mathsf{G}_{2,\hat{\imath},1}$, $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},0}$–$\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},3}$, $\mathsf{G}_{2,\hat{\imath},3}$, $\mathsf{G}_{2,\hat{\imath},4}$, and $\mathsf{G}_{2,\hat{\imath},5}$ for $\hat{\imath} \in \{1,\ldots,L\}$ and $\hat{\jmath} \in \{1,\ldots,\hat{\imath}\alpha\}$, and finally G_3. The hybrids are given in Figs. 5 and 6. A summary can be found in Table 2. They make use of random functions $\mathsf{RF}_{\hat{\imath},\hat{\jmath}} : \{0,1\}^{\hat{\jmath}} \to \mathbb{Z}_q^{1\times 2k}$, $\mathsf{RF}^{(0)}_{\hat{\imath},\hat{\jmath}} : \{0,1\}^{\hat{\jmath}} \to \mathbb{Z}_q^{1\times k}$, and $\mathsf{RF}^{(1)}_{\hat{\imath},\hat{\jmath}} : \{0,1\}^{\hat{\jmath}} \to \mathbb{Z}_q^{1\times k}$, defined on-the-fly. □

Table 2. Summary of the hybrids of Figs. 5 and 6. EVAL queries with $p = \hat{\imath}$ draw $\mathbf{t}$ from the set described by the second column and add the randomness $r_u(\mathsf{m})\,\mathbf{t}$ to u or choose u uniform random. The CHAL query adds the term $r_{\mathbf{h}_0}(\mathsf{m}^\star)^\top$ to $\mathbf{h}_0$ if $\mathsf{m}^\star$ has length $\hat{\imath}$. The column "Transition" displays how we can switch to this hybrid from the previous one. The background colors indicate repeated transitions.

Hybrid	$\mathbf{t}$ uniform in	$r_u(\mathsf{m})$	$r_{\mathbf{h}_0}(\mathsf{m})$	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
$\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},0}$	$\mathbb{Z}_q^{3k}$	$\mathsf{RF}_{\hat{\imath},\hat{\jmath}}\left(\llbracket\mathsf{m}\rrbracket_{\vert\hat{\jmath}}\right)\left(\mathbf{B}^\perp\right)^\top$		Identical

$\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},1}$	**if** $\llbracket\mathsf{m}\rrbracket_{\hat{\jmath}+1} = 0$ **then**
	$\vert$ $\mathsf{Span}(\mathbf{B}\vert\mathbf{B}_0)$
	else
	$\lfloor$ $\mathsf{Span}(\mathbf{B}\vert\mathbf{B}_1)$
		$\mathsf{RF}_{\hat{\imath},\hat{\jmath}}\left(\llbracket\mathsf{m}\rrbracket_{\vert\hat{\jmath}}\right)\left(\mathbf{B}^\perp\right)^\top$		$2 \times \mathcal{U}_k$-MDDH

$\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},2}$		$\Big(\mathsf{RF}^{(0)}_{\hat{\imath},\hat{\jmath}+1}\left(\llbracket\mathsf{m}\rrbracket_{\vert\hat{\jmath}+1}\right)(\mathbf{B}_0^*)^\top + \mathsf{RF}^{(1)}_{\hat{\imath},\hat{\jmath}}\left(\llbracket\mathsf{m}\rrbracket_{\vert\hat{\jmath}}\right)(\mathbf{B}_1^*)^\top\Big)$		Identical
$\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},3}$		$\Big(\mathsf{RF}^{(0)}_{\hat{\imath},\hat{\jmath}+1}\left(\llbracket\mathsf{m}\rrbracket_{\vert\hat{\jmath}+1}\right)(\mathbf{B}_0^*)^\top + \mathsf{RF}^{(1)}_{\hat{\imath},\hat{\jmath}+1}\left(\llbracket\mathsf{m}\rrbracket_{\vert\hat{\jmath}+1}\right)(\mathbf{B}_1^*)^\top\Big)$		Identical
$\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath}+1,3}$	$\mathbb{Z}_q^{3k}$	$\mathsf{RF}_{\hat{\imath},\hat{\jmath}+1}\left(\llbracket\mathsf{m}\rrbracket_{\vert\hat{\jmath}+1}\right)\left(\mathbf{B}^\perp\right)^\top$		$2 \times \mathcal{U}_k$-MDDH
$\mathsf{G}_{2,\hat{\imath},3}$	$\mathbb{Z}_q^{3k}$	uniform random	$\mathsf{RF}_{\hat{\imath}}\left(\mathsf{m}_{\vert\hat{\imath}}\right)\left(\mathbf{B}^\perp\right)^\top$	Identical
$\mathsf{G}_{2,\hat{\imath},4}$	$\mathbb{Z}_q^{3k}$	uniform random	0	Identical
$\mathsf{G}_{2,\hat{\imath},5}$	$\mathsf{Span}(\mathbf{B})$	uniform random	0	$\mathcal{U}_k$-MDDH
G_3	$\mathsf{Span}(\mathbf{B})$	uniform random	0	Statistically close

G_0 | G_1 | $\mathsf{G}_{2,\hat\imath,0}$ | $\mathsf{G}_{2,\hat\imath,1}$ | $\mathsf{G}_{2,\hat\imath,3}$ $\mathsf{G}_{2,\hat\imath,4}$ | $\mathsf{G}_{2,\hat\imath,5}$ | G_3

```
INIT:
$\mathbf{B} \xleftarrow{\$} \mathcal{U}_{3k,k}$
for $i \in \{1,\dots,L\}, j \in \{1,\dots,i\alpha\}$ do
    $\mathbf{x}_{i,j,0}, \mathbf{x}_{i,j,1} \xleftarrow{\$} \mathbb{Z}_q^{3k}$
$x'_0 \xleftarrow{\$} \mathbb{Z}_q$
$K : \mathcal{S}^{\leq L} \dashrightarrow \left(\left(\mathbb{Z}_q^{3k}\right)^{\leq L} \times \mathbb{Z}_q\right)$
$\mathsf{dk} = \left(\left[\mathbf{x}_{i,j,b}^\top \mathbf{B}\right]_2\right)_{1\leq i\leq L, 1\leq j\leq i\alpha, b\in\{0,1\}}$
return $\left([\mathbf{B}]_2, \mathsf{dk}\right)$

CHAL($\mathsf{m}^\star \in \mathcal{S}^p$):            // one query
$h \xleftarrow{\$} \mathbb{Z}_q$
$\mathbf{h}_0 := \left(\sum_{i=1}^{L} \sum_{j=1}^{i\alpha} \mathbf{x}_{i,j,[\![\mathsf{m}^\star]\!]_j}\right) h$
$\boxed{\mathbf{h}_0 \mathrel{+}= \mathbf{B}^\perp \mathsf{RF}_{\hat\imath,\hat\jmath}(\mathsf{m}^\star)^\top h}$
$h_1 := x'_0 \cdot h$
$\boxed{\boxed{h_1 \xleftarrow{\$} \mathbb{Z}_q}}$
return $\left([h], [\mathbf{h}_0]_1, [h_1]_T\right)$

FINALIZE($\beta \in \{0,1\}$):
return $\mathsf{Prefix}(\mathsf{m}^\star) \cap \mathcal{Q}_{\mathcal{M}} = \emptyset) \land \beta$
```

```
EVAL($\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m} \in \mathcal{S}^p$):
$\boxed{\textbf{if } \mathsf{m} \in \mathcal{Q}_{\mathcal{M}} \textbf{ then}}$
    $\boxed{\textbf{return } \mathsf{RerandomizeTag}(K(\mathsf{m}))}$
$\mathcal{Q}_{\mathcal{M}} := \mathcal{Q}_{\mathcal{M}} \cup \{\mathsf{m}\}$
$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k; \mathbf{t} := \mathbf{B}\mathbf{s}$
if $p = \hat\imath$ then $\mathbf{t} \xleftarrow{\$} \mathbb{Z}_q^{3k}$
$u := \left(\sum_{i=1}^{p} \sum_{j=1}^{i\alpha} \mathbf{x}_{i,j,[\![\mathsf{m}]\!]_j}^\top\right) \mathbf{t} + x'_0$
if $p < \hat\imath$ then $u \xleftarrow{\$} \mathbb{Z}_q$
if $p = \hat\imath$ then $u \xleftarrow{\$} \mathbb{Z}_q$
$\boxed{\boxed{u \xleftarrow{\$} \mathbb{Z}_q}}$
for $i \in \{p+1,\dots,L\}, j \in \{1,\dots,i\alpha\}$ do
    $d_{i,j,0} := \mathbf{x}_{i,j,0}^\top \mathbf{t}; d_{i,j,1} := \mathbf{x}_{i,j,1}^\top \mathbf{t}$
$\mathsf{tdk} := \left([d_{i,j,b}]_2\right)_{p+1\leq i\leq L, 1\leq j\leq \ell'(l,i), b\in\{0,1\}}$
$K(\mathsf{m}) := \left([\mathbf{t}]_2, [u]_2, \mathsf{tdk}\right)$
return $K(\mathsf{m})$

RerandomizeTag($\tau$):
Parse $\tau =: \left([\mathbf{t}]_2, [u]_2, \mathsf{tdk}\right)$
$\mathsf{tdk} =: \left([d_{i,j,b}]_2\right)_{p+1\leq i\leq L, 1\leq j\leq \ell'(l,i), b\in\{0,1\}}$
$\mathbf{s}' \xleftarrow{\$} \mathbb{Z}_q^k; \mathbf{t}' := \mathbf{t} + \mathbf{B}\mathbf{s}'$
$u' := u + \sum_{i=1}^{p} \left(\sum_{j=1}^{i\alpha} \mathbf{x}_{i,j,[\![\mathsf{m}]\!]_j}^\top \mathbf{B}\mathbf{s}'\right)$
for $i \in \{p+1,\dots,L\}, j \in \{1,\dots,i\alpha\}$ do
    $d'_{i,j,0} := d_{i,j,0} + \mathbf{x}_{i,j,0}^\top \mathbf{B}\mathbf{s}'$
    $d'_{i,j,1} := d_{i,j,1} + \mathbf{x}_{i,j,1}^\top \mathbf{B}\mathbf{s}'$
$\mathsf{tdk} := \left(\left[d'_{i,j,b}\right]_2\right)_{p+1\leq i\leq L, 1\leq j\leq \ell'(l,i), b\in\{0,1\}}$
return $\left([\mathbf{t}']_2, [u']_2, \mathsf{tdk}\right)$
```

Fig. 5. Hybrids for the security proof of $\mathsf{MAC}_1[\mathcal{U}_{3k,k}]$. The notion $a \mathrel{+}= b$ is shorthand for $a := a + b$. The algorithm $\mathsf{RerandomizeTag}$ is only helper function and not an oracle for the adversary.

Lemma 4 **($\mathsf{G}_0 \rightsquigarrow \mathsf{G}_1$).**

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

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 rerandomized tag is identically distributed to a fresh tag: $\mathbf{t}' := \mathbf{t} + \mathbf{B}\mathbf{s}'$ is uniformly random in $\mathsf{Span}(\mathbf{B})$, when $\mathbf{s}'$ is uniform random in $\mathbb{Z}_q^k$. Together with $u' := u + \sum_{i=1}^{p} \left(\sum_{j=1}^{i\alpha} \mathbf{x}_{i,j,[\![\mathsf{m}]\!]_j}^\top \mathbf{B}\mathbf{s}' \right)$ we get a valid message tag for m, when $([\mathbf{t}]_2, [u]_2)$ is a valid tag for m.

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. To put it in a nutshell, repeated Eval-queries for a message m will leak no information, that is not already leaked by the first Eval-query for m or by the"public key".[4]

□

Lemma 5 ($\mathsf{G}_1 \rightsquigarrow \mathsf{G}_{2,1,0}$).

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

Proof. These two games are equivalent. □

Lemma 6 ($\mathsf{G}_{2,\hat{\imath},0} \rightsquigarrow \mathsf{G}_{2,\hat{\imath},1}$). *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left| \Pr\left[\mathsf{G}_{2,\hat{\imath},0}^{\mathcal{A}} \Rightarrow 1\right] - \Pr[\mathsf{G}_{2,\hat{\imath},1}^{\mathcal{A}} \Rightarrow 1] \right| \leq \mathsf{Adv}_{\mathcal{U}_k,\mathsf{GGen},\mathbb{G}_2}^{\mathsf{mddh}}(\mathcal{B}) + \frac{1}{q-1}$$

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

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 straight forward reduction to the QL-fold $\mathcal{U}_{3k,k}$-MDDH assumption. Remember that by Lemma 1, the $\mathcal{U}_{3k,k}$-MDDH assumption is equivalent to the $\mathcal{U}_k$-MDDH assumption.

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 7 ($\mathsf{G}_{2,\hat{\imath},1} \rightsquigarrow \mathsf{G}_{2,\hat{\imath},3}$). *For all $\hat{\imath} \in \{1, \ldots, L\}$, $\hat{\jmath} \in \{1, \ldots, \hat{\imath}\alpha - 1\}$ and all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left| \Pr\left[\mathsf{G}_{2,\hat{\imath},1}^{\mathcal{A}} \Rightarrow 1\right] - \Pr\left[\mathsf{G}_{2,\hat{\imath},3}^{\mathcal{A}} \Rightarrow 1\right] \right| \leq 4\hat{\imath}\alpha \left(\mathsf{Adv}_{\mathcal{U}_k,\mathsf{GGen},\mathbb{G}_2}^{\mathsf{mddh}}(\mathcal{B}) + \frac{1}{q-1} \right)$$

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

Proof. To prove this transition, we introduce new hybrids $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},1}$, $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},2}$ and $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},3}$ for $\hat{\imath} \in \{1, \ldots, L\}$ and $\hat{\jmath} \in \{1, \ldots, \hat{\imath}\alpha - 1\}$. The hybrids are given in Fig. 6.

Lemma 7 follows directly from Lemmas 8, 9, 10, 11, 12 and 13. □

[4] The same technique can be used to prove the IBE of [3] secure with duplicated Ext-queries. Thus they work without a pseudorandom function.

$\mathsf{G}_{2,\hat\imath,1}$ $\boxed{\mathsf{G}_{2,\hat\imath,2,\hat\jmath,0}}$ $\boxed{\mathsf{G}_{2,\hat\imath,2,\hat\jmath,1}\ \boxed{\mathsf{G}_{2,\hat\imath,2,\hat\jmath,2}}\ \boxed{\mathsf{G}_{2,\hat\imath,2,\hat\jmath,3}}}$ $\boxed{\boxed{\mathsf{G}_{2,\hat\imath,3}}}$

```
INIT:
$\mathbf{B}\ \boxed{\boxed{\boxed{\mathbf{B}_0,\mathbf{B}_1}\ \mathbf{B}_0^*,\mathbf{B}_1^*}} \xleftarrow{\$} \mathcal{U}_{3k,k}$
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 $i \in \{1,\dots,L\}, j \in \{1,\dots,i\alpha\}$ do
    $\mathbf{x}_{i,j,0},\mathbf{x}_{i,j,1} \xleftarrow{\$} \mathbb{Z}_q^{3k}$
$x'_0 \xleftarrow{\$} \mathbb{Z}_q$
$K : \mathcal{S}^{\leq L} \dashrightarrow \Big(\big(\mathbb{Z}_q^{3k}\big)^{\leq L} \times \mathbb{Z}_q\Big)$
$\mathsf{dk} = \Big(\big[\mathbf{x}_{i,j,b}^\top\mathbf{B}\big]_2\Big)_{1\leq i\leq L, 1\leq j\leq i\alpha, b\in\{0,1\}}$
return $\big([\mathbf{B}]_2, \mathsf{dk}\big)$

CHAL($\mathsf{m}^\star \in \mathcal{S}^p$):                // one query
$h \xleftarrow{\$} \mathbb{Z}_q$
$\mathbf{h}_0 := \sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{x}_{i,j,[\![\mathsf{m}^\star]\!]_j} h$
if $\hat\imath \leq p$ then
    $\mathbf{h}_0 := \mathbf{h}_0$
        $+\ \mathbf{B}^\perp\mathsf{RF}_{\hat\imath,\hat\jmath}\big([\![\mathsf{m}^\star]\!]_{|\hat\jmath}\big)^\top h$
        $+\ \Big(\mathbf{B}_0^*\mathsf{RF}^{(0)}_{\hat\imath,\hat\jmath+1}\big([\![\mathsf{m}^\star]\!]_{|\hat\jmath+1}\big)^\top + \mathbf{B}_1^*\mathsf{RF}^{(1)}_{\hat\imath,\hat\jmath}\big([\![\mathsf{m}^\star]\!]_{|\hat\jmath}\big)^\top\Big)h$
        $+\ \Big(\mathbf{B}_0^*\mathsf{RF}^{(0)}_{\hat\imath,\hat\jmath+1}\big([\![\mathsf{m}^\star]\!]_{|\hat\jmath+1}\big)^\top + \mathbf{B}_1^*\mathsf{RF}^{(1)}_{\hat\imath,\hat\jmath+1}\big([\![\mathsf{m}^\star]\!]_{|\hat\jmath+1}\big)^\top\Big)h$
$h_1 := x'_0 \cdot h$
return $\big([h], [\mathbf{h}_0]_1, [h_1]_T\big)$

FINALIZE($\beta \in \{0,1\}$):
return $\mathsf{Prefix}(\mathsf{m}^\star) \cap \mathcal{Q}_\mathcal{M} = \emptyset) \wedge \beta$
```

```
EVAL($\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m} \in \mathcal{S}^p$):
if $\mathsf{m} \in \mathcal{Q}_\mathcal{M}$ then
    return $\mathsf{RerandomizeTag}(K(\mathsf{m}))$
$\mathcal{Q}_\mathcal{M} := \mathcal{Q}_\mathcal{M} \cup \{\mathsf{m}\}$
$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{t} := \mathbf{Bs}$
if $p = \hat\imath$ then
    $\mathbf{t} \xleftarrow{\$} \mathbb{Z}_q^{3k}$
    $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^{2k}$
    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
    $u \xleftarrow{\$} \mathbb{Z}_q$
else
    $u := \Big(\sum_{i=1}^{p}\sum_{j=1}^{i\alpha} \mathbf{x}_{i,j,[\![\mathsf{m}]\!]_j}^\top\Big)\mathbf{t} + x'_0$
if $p = \hat\imath$ then
    $u := u$
        $+\ \mathsf{RF}_{\hat\imath,\hat\jmath}\big([\![\mathsf{m}]\!]_{|\hat\jmath}\big)\big(\mathbf{B}^\perp\big)^\top\mathbf{t}$
        $+\ \Big(\mathsf{RF}^{(0)}_{\hat\imath,\hat\jmath+1}\big([\![\mathsf{m}]\!]_{|\hat\jmath+1}\big)(\mathbf{B}_0^*)^\top + \mathsf{RF}^{(1)}_{\hat\imath,\hat\jmath}\big([\![\mathsf{m}]\!]_{|\hat\jmath}\big)(\mathbf{B}_1^*)^\top\Big)\mathbf{t}$
        $+\ \Big(\mathsf{RF}^{(0)}_{\hat\imath,\hat\jmath+1}\big([\![\mathsf{m}]\!]_{|\hat\jmath+1}\big)(\mathbf{B}_0^*)^\top + \mathsf{RF}^{(1)}_{\hat\imath,\hat\jmath+1}\big([\![\mathsf{m}]\!]_{|\hat\jmath+1}\big)(\mathbf{B}_1^*)^\top\Big)\mathbf{t}$
    $\boxed{\boxed{u \xleftarrow{\$} \mathbb{Z}_q}}$
for $i \in \{p+1,\dots,L\}, j \in \{1,\dots,i\alpha\}$ do
    $d_{i,j,0} := \mathbf{x}_{i,j,0}^\top\mathbf{t}$; $d_{i,j,1} := \mathbf{x}_{i,j,1}^\top\mathbf{t}$
$\mathsf{tdk} := \big([d_{i,j,b}]_2\big)_{p+1\leq i\leq L, 1\leq j\leq \ell'(l,i), b\in\{0,1\}}$
$K(\mathsf{m}) := \big([\mathbf{t}]_2, [u]_2, \mathsf{tdk}\big)$
return $K(\mathsf{m})$
```

Fig. 6. Hybrids for the transition from $\mathsf{G}_{2,\hat\imath,\hat\jmath}$ to $\mathsf{G}_{2,\hat\imath,\hat\jmath+1}$. The notion $a \mathrel{+}= b$ is shorthand for $a := a + b$. The algorithm $\mathsf{RerandomizeTag}$ is defined in Fig. 5.

Lemma 8 $(\mathsf{G}_{2,\hat{\imath},1} \rightsquigarrow \mathsf{G}_{2,\hat{\imath},2,0,0})$.

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

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

Lemma 9 $(\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},0} \rightsquigarrow \mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},1})$. *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},2,\hat{\jmath},0} \Rightarrow 1\right] - \Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},2,\hat{\jmath},1} \Rightarrow 1\right]\right| \leq 2\left(\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{GGen},\mathbb{G}_2}(\mathcal{B}) + \frac{1}{q-1}\right)$$

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

Proof. These two games are equivalent except that the value $\mathbf{t}$ 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-fold $\mathcal{U}_{3k,k}$-MDDH challenges. Remember that the $\mathcal{U}_{3k,k}$-MDDH assumption is equivalent to the $\mathcal{U}_k$-MDDH assumption by Lemma 1.

To achieve that, we first switch $\mathbf{t}$ for $[\![\mathsf{m}]\!]_{\hat{\jmath}+1} = 0$ 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 $\mathbf{B}_0$ via the MDDH assumption. More precisely, let $([\mathbf{B}_0]_2, [\mathbf{Z}]_2) \in \mathbb{G}_2^{3k\times(k+Q)}$ be a Q-fold $\mathcal{U}_{3k,k}$-MDDH challenge. For the i-th EVAL query with $[\![\mathsf{m}]\!]_{\hat{\jmath}+1} = 0$, the reduction $\mathcal{B}$ computes $[\mathbf{t}]_2 := [\mathbf{B}\mathbf{s}_1 + \mathbf{Z}[i]]_2$, where $\mathbf{s}_1 \xleftarrow{\$} \mathbb{Z}_q^k$ and $\mathbf{Z}[i]$ is the i-th column vector of $\mathbf{Z}$. Furthermore, in order to make sure that the column vectors of $(\mathbf{B}|\mathbf{B}_0|\mathbf{B}_1)$ form a random basis of $\mathbb{Z}_q^{3k}$, the reduction $\mathcal{B}$ chooses $\mathbf{B}, \mathbf{B}_1 \xleftarrow{\$} \mathcal{U}_{3k,k}$ such that $(\mathbf{B}|\mathbf{B}_1)$ has rank $2k$ and $(\mathbf{B}|\mathbf{B}_1)^{\perp}\mathbf{b} = \mathbf{0}$ for all column vectors $\mathbf{b}$ of $\mathbf{B}_0$. We note that the latter one can be done over group $\mathbb{G}_2$ by knowing $\mathbf{B}$ and $\mathbf{B}_1$ over $\mathbb{Z}_q$.

Until now, if $\mathbf{Z}$ is uniform then $\mathcal{B}$ simulates the game $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},0}$, else if $\mathbf{Z}$ is from $\mathsf{Span}(\mathbf{B}_0)$ then $\mathcal{B}$ simulates the game $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},1}$ for messages with $[\![\mathsf{m}]\!]_{\hat{\jmath}+1} = 0$.

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

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 10 $(\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},1} \rightsquigarrow \mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},2})$.

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

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 $\mathsf{RF}^{(0)}_{\hat{\imath},\hat{\jmath}+1}\left(\llbracket\mathsf{m}\rrbracket_{|\hat{\jmath}+1}\right)(\mathbf{B}_0^*)^{\top} + \mathsf{RF}^{(1)}_{\hat{\imath},\hat{\jmath}}\left(\llbracket\mathsf{m}\rrbracket_{|\hat{\jmath}}\right)(\mathbf{B}_1^*)^{\top}$. 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

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

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

The Eval-queries with $p \neq \hat{\imath}$ use the same code in both games and Eval-queries with $p = \hat{\imath}$ and $\llbracket\mathsf{m}\rrbracket_{\hat{\jmath}+1} = 0$ are distributed identically in both games, by definition of $\mathsf{RF}^{(0)}_{\hat{\imath},\hat{\jmath}+1}$.

The 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 $\mathbf{B}_0^*$ and thus $\mathsf{RF}^{(0)}_{\hat{\imath},\hat{\jmath}+1}\left(\llbracket\mathsf{m}\rrbracket_{|\hat{\jmath}+1}\right)(\mathbf{B}_0^*)^{\top}\mathbf{t} = 0$.

The Chal query uses the same code if $p \neq \hat{\imath}$ and otherwise it is distributed identically if $\llbracket\mathsf{m}^\star\rrbracket_{\hat{\jmath}+1} = 0$. For the case $\llbracket\mathsf{m}^\star\rrbracket_{\hat{\jmath}+1} = 1$ note that $\mathbf{x}_{\hat{\imath},\hat{\jmath}+1,1}$ is identically distributed as $\mathbf{x}_{\hat{\imath},\hat{\jmath}+1,1} + \mathbf{B}_0^*\mathbf{w}$ for $\mathbf{w} \overset{\$}{\leftarrow} \mathbb{Z}_q^k$ and $\mathbf{w}$ is hidden from the adversary except for the Chal query: In all Eval-queries with $p \neq \hat{\imath}$ only $\mathbf{x}_{\hat{\imath},\hat{\jmath}+1,1}\mathbf{B}$ is used and thus the $\mathbf{B}_0^*$-part cancels out. In the Eval-queries with $p = \hat{\imath}$ there is either $\llbracket\mathsf{m}\rrbracket_{\hat{\jmath}+1} = 0$ which means that $\mathbf{x}_{\hat{\imath},\hat{\jmath}+1,1}$ is not used to compute the tag or there is $\llbracket\mathsf{m}\rrbracket_{\hat{\jmath}+1} = 1$ which means that $\mathbf{t} \in \mathsf{Span}(\mathbf{B}|\mathbf{B}_1)$ and thus the $\mathbf{B}_0^*$ -part of $\mathbf{x}_{\hat{\imath},\hat{\jmath}+1,1}$ cancels out. All in all this means that the value $\mathbf{h}_0$ is the only one in the game that depends on $\mathbf{w}$ and thus the $\mathbf{B}_0^*$-part of $\mathbf{h}_0$ is uniformly random to the adversary. Especially $\mathbf{h}_0$ is distributed identically in both games. □

Lemma 11 ($\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},2} \rightsquigarrow \mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},3}$)**.**

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

Proof. We define

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

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

The argument, that the games $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},2}$ and $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},3}$ are identically distributed, is the same as in Lemma 10, just with the roles of 0 and 1 swapped. □

Lemma 12 ($\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},3} \rightsquigarrow \mathsf{G}_{2,\hat{\imath},2,\hat{\jmath}+1,0}$)**.** *For $\hat{\jmath} < \hat{\imath}\alpha$ and all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},2,\hat{\jmath},3} \Rightarrow 1\right] - \Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},\hat{\jmath}+1} \Rightarrow 1\right]\right| \leq 2\left(\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{GGen},\mathbb{G}_2}(\mathcal{B}) + \frac{1}{q-1}\right)$$

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

Proof. The transition is the reverse of Lemma 9. □

Lemma 13 ($\mathsf{G}_{2,\hat{\imath},2,\hat{\imath}\alpha,3} \rightsquigarrow \mathsf{G}_{2,\hat{\imath},3}$)**.**

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

Proof. In game $\mathsf{G}_{2,\hat{\imath},2,\hat{\imath}\alpha,3}$ the Chal-query evaluates $\mathsf{RF}_{\hat{\imath},\hat{\imath}\alpha}$ only for the input value $\mathsf{m}^\star_1||\ldots||\mathsf{m}^\star_{\hat{\imath}}$ (if $p \geq \hat{\imath}$, otherwise it does not use $\mathsf{RF}_{\hat{\imath},\hat{\imath}\alpha}$ at all). Assume $\mathsf{Prefix}(\mathsf{m}^\star) \cap \mathcal{Q}_{\mathcal{M}} = \emptyset$, 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 part of 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. Thus each query outputs a uniformly random value for u when $\mathbf{t}_p \notin \mathsf{Span}(\mathbf{B})$, which happens with probability $\geq 1 - 1/\left(q^{2k}\right)$. In this case the games are distributed identically. □

Lemma 14 ($\mathsf{G}_{2,\hat{\imath},3} \rightsquigarrow \mathsf{G}_{2,\hat{\imath},4}$)**.**

$$\Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},3} \Rightarrow 1\right] = \Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},4} \Rightarrow 1\right]$$

Proof. The games execute the same code if $p < \hat{\imath}$ and otherwise we can argue that $\mathbf{x}_{\hat{\imath},1,[\![\mathsf{m}^\star]\!]_1}$ and $\mathbf{x}_{\hat{\imath},1,[\![\mathsf{m}^\star]\!]_1} - \mathbf{B}^\perp\left(\mathsf{RF}_{\hat{\imath},\hat{\imath}\alpha}(\mathsf{m}^\star)\right)^\top$ are identical distributed. All Eval-queries and the "public key" returned by Init make only use of $\mathbf{x}_{\hat{\imath},1,[\![\mathsf{m}^\star]\!]_1}\mathbf{B}$, so the $\mathbf{B}^\perp\left(\mathsf{RF}_{\hat{\imath},\hat{\imath}\alpha}(\cdot)\right)^\top$ part cancels out. □

Lemma 15 ($\mathsf{G}_{2,\hat{\imath},4} \rightsquigarrow \mathsf{G}_{2,\hat{\imath},5}$)**.** *For all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

$$\left|\Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},4} \Rightarrow 1\right] - \Pr\left[\mathsf{G}^{\mathcal{A}}_{2,\hat{\imath},5} \Rightarrow 1\right]\right| \leq \mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{GGen},\mathbb{G}_2}(\mathcal{B}) + \frac{1}{q-1}$$

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

Proof. The transition is the reverse of Lemma 6. □

Lemma 16 ($\mathsf{G}_{2,\hat{\imath},5} \rightsquigarrow \mathsf{G}_{2,\hat{\imath}+1,0}$)**.** *For $\hat{\imath} < L$*

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

Proof. These two games are equivalent. □

Lemma 17 $(\mathsf{G}_{2,L,5} \rightsquigarrow \mathsf{G}_3)$**.**

$$\Pr\left[\mathsf{G}_{2,L,5}^{\mathcal{A}} \Rightarrow 1\right] = \Pr\left[\mathsf{G}_{3}^{\mathcal{A}} \Rightarrow 1\right].$$

Proof. In game $\mathsf{G}_{2,L,5}$ the value x_0' is only used to compute h_1, thus h_1 is a uniform random value to $\mathcal{A}$ and the games are distributed identical. □

Summary. To prove Theorem 1 combine Lemmas 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 and 17 to change h_1 from real to random and then apply all Lemmas in reverse order to get to the $\mathsf{HPR}_0\text{-}\mathsf{CMA}_{\mathsf{rand}}$ game. □

3.2 Our Second Construction

Let $(\mathbb{G}_2, q, P_2)$ be a group of prime order q. Our second affine MAC with levels $\mathsf{MAC}_1[\mathcal{U}_{3k,k}] := (\mathsf{Gen}_{\mathsf{MAC}}, \mathsf{Tag}, \mathsf{Ver}_{\mathsf{MAC}})$ with message space $\mathcal{ID} := \mathcal{S}^{\leq L} := (\{0,1\}^{\alpha})^{\leq L}$ is defined in Fig. 7. The identity vectors bit-length α and the maximum length L of the identity vectors can be chosen freely. The difference to the first construction is that this MAC uses a different $\mathbf{t}_l$ on each level ($\ell(p) = p$) and thus needs no delegation keys. This leads to shorter user secret keys and allows a more efficient reduction. However, this comes at the price of larger ciphertexts. Formally, this MAC uses $\ell'(l,i) = 0$ for $i < p$ and $\ell'(l,i) = 2i\alpha$ for $i = p$.

```
$\mathsf{Gen}_{\mathsf{MAC}}(\mathbb{G}_2, q, P_2)$:
$\mathbf{B} \xleftarrow{\$} \mathcal{U}_{3k,k}$
for $i \in \{1,\dots,L\}, j \in \{1,\dots,i\alpha\}, b \in \{0,1\}$ do $\mathbf{x}_{i,j,b} \xleftarrow{\$} \mathbb{Z}_q^{3k}$
$x_0' \xleftarrow{\$} \mathbb{Z}_q$
return $\mathsf{sk}_{\mathsf{MAC}} := \left(\mathbf{B}, (\mathbf{x}_{i,j,b})_{1\leq i\leq L, 1\leq j\leq i\alpha, b\in\{0,1\}}, x_0'\right)$

$\mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m} \in \mathcal{S}^p)$:
Parse $\mathsf{sk}_{\mathsf{MAC}} =: \left(\mathbf{B}, (\mathbf{x}_{i,j,b})_{1\leq i\leq L, 1\leq j\leq i\alpha, b\in\{0,1\}}, x_0'\right)$
for $i \in \{1,\dots,p\}$ do $\mathbf{s}_i \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{t}_i := \mathbf{B}\mathbf{s}_i$
$u := \sum_{i=1}^{p}\left(\sum_{j=1}^{i\alpha} \mathbf{x}_{i,j,\llbracket \mathsf{m} \rrbracket_j}^\top\right)\mathbf{t}_i + x_0'$
return $\left(\left([\mathbf{t}_i]_2\right)_{1\leq i\leq p}, [u]_2\right)$

$\mathsf{Ver}_{\mathsf{MAC}}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m} \in \mathcal{S}^p, \tau)$:
Parse $\mathsf{sk}_{\mathsf{MAC}} =: \left(\mathbf{B}, (\mathbf{x}_{i,j,b})_{1\leq i\leq L, 1\leq j\leq i\alpha, b\in\{0,1\}}, x_0'\right)$
Parse $\mathsf{m} =: (\mathsf{m}_1, \dots, \mathsf{m}_p)$
Parse $\tau =: \left(\left([\mathbf{t}_i]_2\right)_{1\leq i\leq p}, [u]_2\right)$
return $u \stackrel{?}{=} \sum_{i=1}^{p}\left(\sum_{j=1}^{i\alpha} \mathbf{x}_{i,j,\llbracket \mathsf{m} \rrbracket_j}^\top\right)\mathbf{t}_i + x_0'$
```

Fig. 7. Our second affine MAC with levels based on [11]

Theorem 2 (Security of $\mathsf{MAC}_2[\mathcal{U}_{3k,k}]$). $\mathsf{MAC}_2[\mathcal{U}_{3k,k}]$ *is tightly* HPR_0-CMA *secure in* $\mathbb{G}_2$ *under the* $\mathcal{U}_k$-MDDH *assumption for* $\mathbb{G}_2$*. Precisely, for all adversaries* $\mathcal{A}$ *there exists an adversary* $\mathcal{B}$ *with*

$$\mathsf{Adv}^{\mathsf{hpr}_0\text{-}\mathsf{cma}}_{\mathsf{MAC}_2[\mathcal{U}_{3k,k}],\mathbb{G}_2}(\mathcal{A}) \leq (2+8\alpha L)\left(\mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{U}_k,\mathsf{GGen},\mathbb{G}_2}(\mathcal{B}) + \frac{1}{q-1}\right) + \frac{Q}{q^{2k}}$$

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

The proof uses a hybrid argument with the hybrids G_0 (the HPR_0-$\mathsf{CMA}_{\mathsf{real}}$ game), G_1, G_2, $\mathsf{G}_{3,\hat{\jmath}}$ for $\hat{\jmath} \in \{1,\ldots,L\alpha\}$, $\mathsf{G}_{3,\hat{\jmath},1}$–$\mathsf{G}_{3,\hat{\jmath},3}$ for $\hat{\jmath} \in \{1,\ldots,L\alpha-1\}$, and finally G_4. The hybrids are given in Figs. 8 and 9. A summary can be found in Table 3.

The arguments to switch between the hybrids are similar to the first construction. A detailed proof can be found in the full version.

Table 3. Summary of the hybrids of Figs. 8 and 9. Eval queries draw $\mathbf{t}$ from the set described by the second column and add the randomness $\sum_{i=1}^{p} r_u(\mathsf{m},i)\,\mathbf{t}_i$ to u or choose 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 $g(\hat{j},i) := \max\{\hat{\jmath}, i\alpha\}$. The background color indicates repeated transitions.

Hybrid	$\mathbf{t}_i$ uniform in	$r_u(\mathsf{m},i)$	$r_{\mathbf{h}_0}(\mathsf{m},i)$	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
$\mathsf{G}_{3,\hat{\jmath}}$	$\mathbb{Z}_q^{3k}$	$\mathsf{RF}_{i,\hat{\jmath}}\left(\llbracket\mathsf{m}\rrbracket_{\vert g(\hat{\jmath},i)}\right)\left(\mathbf{B}^{\perp}\right)^{\top}$		Identical

$\mathsf{G}_{3,\hat{\jmath},1}$	**if** $\llbracket\mathsf{m}\rrbracket_{\hat{\jmath}+1} = 0$ **then**
	$\vert$ $\mathsf{Span}(\mathbf{B}\vert\mathbf{B}_0)$
	else
	$\lfloor$ $\mathsf{Span}(\mathbf{B}\vert\mathbf{B}_1)$
		$\mathsf{RF}_{i,\hat{\jmath}}\left(\llbracket\mathsf{m}\rrbracket_{\vert g(\hat{\jmath},i)}\right)\left(\mathbf{B}^{\perp}\right)^{\top}$		$2 \times \mathcal{U}_k$-MDDH

$\mathsf{G}_{3,\hat{\jmath},2}$		$\mathsf{RF}^{(0)}_{i,\hat{\jmath}+1}\left(\llbracket\mathsf{m}\rrbracket_{\vert g(\hat{\jmath}+1,i)}\right)(\mathbf{B}_0^*)^{\top}$ $+\,\mathsf{RF}^{(1)}_{i,\hat{\jmath}}\left(\llbracket\mathsf{m}\rrbracket_{\vert g(\hat{\jmath},i)}\right)(\mathbf{B}_1^*)^{\top}$		Identical
$\mathsf{G}_{3,\hat{\jmath},3}$		$\mathsf{RF}^{(0)}_{i,\hat{\jmath}+1}\left(\llbracket\mathsf{m}\rrbracket_{\vert g(\hat{\jmath}+1,i)}\right)(\mathbf{B}_0^*)^{\top}$ $+\,\mathsf{RF}^{(1)}_{i,\hat{\jmath}+1}\left(\llbracket\mathsf{m}\rrbracket_{\vert g(\hat{\jmath}+1,i)}\right)(\mathbf{B}_1^*)^{\top}$		Identical
G_4	$\mathbb{Z}_q^{3k}$	unif. random	$\mathsf{RF}_{i,i\alpha}\left(\mathsf{m}_{\vert i}\right)\left(\mathbf{B}^{\perp}\right)^{\top}$	Statistically close

G_0 G_1 G_2 $\mathsf{G}_{3,\hat{\jmath}}$ G_4

```
INIT:
$\mathbf{B} \xleftarrow{\$} \mathcal{U}_{3k,k}$
for $i \in \{1, \dots, L\}, j \in \{1, \dots, i\alpha\}$ do
    $\mathbf{x}_{i,j,0}, \mathbf{x}_{i,j,1} \xleftarrow{\$} \mathbb{Z}_q^{3k}$
$x'_0 \xleftarrow{\$} \mathbb{Z}_q$
$K : \mathcal{S}^{\leq L} \dashrightarrow \left( \left( \mathbb{Z}_q^{3k} \right)^{\leq L} \times \mathbb{Z}_q \right)$
$\mathsf{dk} = \left( \left[ \mathbf{x}_{i,j,b}^\top \mathbf{B} \right]_2 \right)_{1 \leq i \leq L, 1 \leq j \leq i\alpha, b \in \{0,1\}}$
return $\left( [\mathbf{B}]_2, \mathsf{dk} \right)$

CHAL($\mathsf{m}^\star \in \mathcal{S}^p$):                    // one query
$h \xleftarrow{\$} \mathbb{Z}_q$
for $i \in \{1, \dots, p\}$ do
    $\mathbf{h}_{0,i} := \sum_{j=1}^{i\alpha} \mathbf{x}_{i,j,\llbracket \mathsf{m}^\star \rrbracket_j} h$
$\hat{\jmath} := L\alpha$
$\hat{\imath} := \lfloor (\hat{\jmath} + 1)/\alpha \rfloor$
for $i \in \{1, \dots, \min\{p, \hat{\imath} - 1\}\}$ do
    $\mathbf{h}_{0,i} \mathrel{+}= \mathbf{B}^\perp \mathsf{RF}_{i,i\alpha} \left( \left\llbracket \mathsf{m}^\star_{|i} \right\rrbracket \right)^\top h$
for $i \in \{\hat{\imath}, \dots, p\}$ do
    $\mathbf{h}_{0,i} \mathrel{+}= \mathbf{B}^\perp \mathsf{RF}_{i,\hat{\jmath}} \left( \llbracket \mathsf{m}^\star \rrbracket_{|\hat{\jmath}} \right)^\top h$
$h_1 := x'_0 \cdot h$
$h_1 \xleftarrow{\$} \mathbb{Z}_q$
return $\left( [h], \left( [\mathbf{h}_{0,i}]_1 \right)_{1 \leq i \leq p}, [h_1]_T \right)$

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

EVAL($\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m} \in \mathcal{S}^p$):
if $\mathsf{m} \in \mathcal{Q}_{\mathcal{M}}$ then
    return $\mathsf{RerandomizeTag}(K(\mathsf{m}))$
$\mathcal{Q}_{\mathcal{M}} := \mathcal{Q}_{\mathcal{M}} \cup \{\mathsf{m}\}$
for $i \in \{1, \dots, p\}$ do
    $\mathbf{s}_i \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{t}_i := \mathbf{B}\mathbf{s}_i$
    $\mathbf{t}_i \xleftarrow{\$} \mathbb{Z}_q^{3k}$
for $i \in \{1, \dots, p\}$ do
    $u_i := \sum_{j=1}^{i\alpha} \mathbf{x}_{i,j,\llbracket \mathsf{m} \rrbracket_j}^\top \mathbf{t}_i$
$\hat{\imath} := \lfloor (\hat{\jmath} + 1)/\alpha \rfloor$
for $i \in \{1, \dots, \min\{p, \hat{\imath} - 1\}\}$ do
    $u_i \mathrel{+}= \mathsf{RF}_{i,i\alpha} \left( \llbracket \mathsf{m}_{|i} \rrbracket \right) \left( \mathbf{B}^\perp \right)^\top \mathbf{t}_i$
for $i \in \{\hat{\imath}, \dots, p\}$ do
    $u_i \mathrel{+}= \mathsf{RF}_{i,\hat{\jmath}} \left( \llbracket \mathsf{m} \rrbracket_{|\hat{\jmath}} \right) \left( \mathbf{B}^\perp \right)^\top \mathbf{t}_i$
$u := \sum_{i=1}^p u_i + x'_0$
$u \xleftarrow{\$} \mathbb{Z}_q$
$K(\mathsf{m}) := \left( \left( [\mathbf{t}_i]_2 \right)_{1 \leq i \leq p}, [u]_2 \right)$
return $K(\mathsf{m})$

RerandomizeTag($\tau$):
Parse $\tau =: \left( \left( [\mathbf{t}_i]_2 \right)_{1 \leq i \leq p}, [u]_2 \right)$
for $i \in \{1, \dots, p\}$ do
    $\mathbf{s}'_i \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{t}'_i := \mathbf{t}_i + \mathbf{B}\mathbf{s}'_i$
$u' := u + \sum_{i=1}^p \left( \sum_{j=1}^{i\alpha} \mathbf{x}_{i,j,\llbracket \mathsf{m} \rrbracket_j}^\top \mathbf{B}\mathbf{s}'_i \right)$
return $\left( \left( [\mathbf{t}'_i]_2 \right)_{1 \leq i \leq p}, [u']_2 \right)$
```

Fig. 8. Hybrids for the security proof of $\mathsf{MAC}_2[\mathcal{U}_{3k,k}]$. The notion $a \mathrel{+}= b$ is shorthand for $a := a + b$.

$\mathsf{G}_{3,\hat{\jmath}}$ $\boxed{\mathsf{G}_{3,\hat{\jmath},1}}$ $\boxed{\mathsf{G}_{3,\hat{\jmath},2}}$ $\boxed{\mathsf{G}_{3,\hat{\jmath},3}}$

```
INIT:
$\mathbf{B}\ \boxed{\boxed{\boxed{\mathbf{B}_0,\mathbf{B}_1}\ \mathbf{B}_0^*,\mathbf{B}_1^*}} \xleftarrow{\$} \mathcal{U}_{3k,k}$
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 $\mathsf{Span}(\mathbf{B}^\perp)$
  – $\mathbf{B}_1^\top\mathbf{B}_0^* = \mathbf{B}_0^\top\mathbf{B}_1^*$
for $i \in \{1,\dots,L\}, j \in \{1,\dots,i\alpha\}$ do
    $\mathbf{x}_{i,j,0},\mathbf{x}_{i,j,1} \xleftarrow{\$} \mathbb{Z}_q^{3k}$
$x_0' \xleftarrow{\$} \mathbb{Z}_q$
$K : \mathcal{S}^{\le L} \dashrightarrow \left(\left(\mathbb{Z}_q^{3k}\right)^{\le L} \times \mathbb{Z}_q\right)$
$\mathsf{dk} = \left(\left[\mathbf{x}_{i,j,b}^\top\mathbf{B}\right]_2\right)_{1\le i\le L, 1\le j\le i\alpha, b\in\{0,1\}}$
return $\left([\mathbf{B}]_2, \mathsf{dk}\right)$

CHAL($\mathsf{m}^\star \in \mathcal{S}^p$):                    // one query
$h \xleftarrow{\$} \mathbb{Z}_q$
for $i \in \{1,\dots,p\}$ do
    $\mathbf{h}_{0,i} := \sum_{j=1}^{i\alpha} \mathbf{x}_{i,j,\llbracket \mathsf{m}^\star\rrbracket_j} h$
for $i \in \{1,\dots,\min\{p,\hat{\imath}-1\}\}$ do
    $\mathbf{h}_{0,i} \mathrel{+}= \mathsf{RF}_{i,i\alpha}\left(\left\llbracket \mathsf{m}^\star_{|i}\right\rrbracket\right)\left(\mathbf{B}^\perp\right)^\top h$
$\hat{\imath} := \lfloor(\hat{\jmath}+1)/\alpha\rfloor$
for $i \in \{\hat{\imath},\dots,p\}$ do
    $\mathbf{h}_{0,\hat{\imath}} := \mathbf{h}_{0,\hat{\imath}}$
    $\boxed{+\ \mathbf{B}^\perp\mathsf{RF}_{i,\hat{\jmath}}\left(\llbracket\mathsf{m}^\star\rrbracket_{|\hat{\jmath}}\right)^\top h}$
    $\boxed{+\left(\mathbf{B}_0^*\mathsf{RF}^{(0)}_{i,\hat{\jmath}+1}\left(\llbracket\mathsf{m}^\star\rrbracket_{|\hat{\jmath}+1}\right)^\top + \mathbf{B}_1^*\mathsf{RF}^{(1)}_{i,\hat{\jmath}}\left(\llbracket\mathsf{m}^\star\rrbracket_{|\hat{\jmath}}\right)^\top\right)h}$
    $\boxed{+\left(\mathbf{B}_0^*\mathsf{RF}^{(0)}_{i,\hat{\jmath}+1}\left(\llbracket\mathsf{m}^\star\rrbracket_{|\hat{\jmath}+1}\right)^\top + \mathbf{B}_1^*\mathsf{RF}^{(1)}_{i,\hat{\jmath}+1}\left(\llbracket\mathsf{m}^\star\rrbracket_{|\hat{\jmath}+1}\right)^\top\right)h}$
$h_1 := x_0' \cdot h$
return $\left([h], \left([\mathbf{h}_{0,i}]_1\right)_{1\le i\le p}, [h_1]_T\right)$

FINALIZE($\beta \in \{0,1\}$):
return  $\mathsf{Prefix}(\mathsf{m}^\star) \cap \mathcal{Q}_{\mathcal{M}} = \emptyset) \wedge \beta$
```

```
EVAL($\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m} \in \mathcal{S}^p$):
Parse $\mathsf{m} =: (\mathsf{m}_1,\dots,\mathsf{m}_p)$
if $\mathsf{m} \in \mathcal{Q}_{\mathcal{M}}$ then
    if $\mathsf{m} \in \mathcal{Q}_{\mathcal{M}}$ then
        return $\mathsf{RerandomizeTag}(K(\mathsf{m}))$
$\mathcal{Q}_{\mathcal{M}} := \mathcal{Q}_{\mathcal{M}} \cup \{\mathsf{m}\}$
for $i \in \{1,\dots,p\}$ do  $\mathbf{t}_i \xleftarrow{\$} \mathbb{Z}_q^{3k}$
$\hat{\imath} := \lfloor(\hat{\jmath}+1)/\alpha\rfloor$
$\boxed{\boxed{\boxed{
for $i \in \{\hat{\imath},\dots,p\}$ do
    $\mathbf{s}_i \xleftarrow{\$} \mathbb{Z}_q^{2k}$
    if $\llbracket\mathsf{m}\rrbracket_{\hat{\jmath}+1} = 0$ then
        $\mathbf{t}_i := (\mathbf{B}|\mathbf{B}_0)\mathbf{s}_i$
    else
        $\mathbf{t}_i := (\mathbf{B}|\mathbf{B}_1)\mathbf{s}_i$
}}}$
for $i \in \{1,\dots,p\}$ do
    $u_i := \sum_{j=1}^{i\alpha} \mathbf{x}_{i,j,\llbracket\mathsf{m}\rrbracket_j}^\top \mathbf{t}_i$
for $i \in \{1,\dots,\min\{p,\hat{\imath}-1\}\}$ do
    $u_i := u_i + \mathsf{RF}_{i,i\alpha}\left(\llbracket\mathsf{m}_{|\hat{\imath}}\rrbracket\right)\left(\mathbf{B}^\perp\right)^\top\mathbf{t}_i$
for $i \in \{\hat{\imath},\dots,p\}$ do
    $u_{\hat{\imath}} := u_{\hat{\imath}}$
    $\boxed{+\ \mathbf{B}^\perp\mathsf{RF}_{i,\hat{\jmath}}\left(\llbracket\mathsf{m}\rrbracket_{|\hat{\jmath}}\right)^\top\mathbf{t}_i}$
    $\boxed{+\left(\mathsf{RF}^{(0)}_{i,\hat{\jmath}+1}\left(\llbracket\mathsf{m}\rrbracket_{|\hat{\jmath}+1}\right)(\mathbf{B}_0^*)^\top + \mathsf{RF}^{(1)}_{i,\hat{\jmath}}\left(\llbracket\mathsf{m}\rrbracket_{|\hat{\jmath}}\right)(\mathbf{B}_1^*)^\top\right)\mathbf{t}_i}$
    $\boxed{+\left(\mathsf{RF}^{(0)}_{i,\hat{\jmath}+1}\left(\llbracket\mathsf{m}\rrbracket_{|\hat{\jmath}+1}\right)(\mathbf{B}_0^*)^\top + \mathsf{RF}^{(1)}_{i,\hat{\jmath}+1}\left(\llbracket\mathsf{m}\rrbracket_{|\hat{\jmath}+1}\right)(\mathbf{B}_1^*)^\top\right)\mathbf{t}_i}$
$u := \sum_{i=1}^p u_i + x_0'$
$K(\mathsf{m}) := \left(\left([\mathbf{t}_i]_2\right)_{1\le i\le p}, [u]_2\right)$
return $K(\mathsf{m})$
```

Fig. 9. Hybrids for the transition from $\mathsf{G}_{3,\hat{\jmath}}$ to $\mathsf{G}_{3,\hat{\jmath}+1}$. The notion $a \mathrel{+}= b$ is shorthand for $a := a + b$.

4 Transformation to HIBE

Any affine MAC with levels can be transformed tightly to a hierarchical identity-based key encapsulation mechanism (HIBKEM) under the $\mathcal{D}_k$-MDDH assumption. The transformation is shown in Fig. 10. It is a generalization of the transformation from delegatable, affine MACs to HIBKEMs in [3]. We only consider HIBKEM here and one can easily prove that every HIBKEM can be transformed (tightly) into an HIBE scheme with a (one-time secure) symmetric cipher by adapting a similar transformation for public-key encryption in [20].

Theorem 3 (Security of the HIBKEM transformation). *The HIBKEM* $\mathsf{HIBKEM}[\mathsf{MAC}, \mathcal{D}_k]$ *is* IND-HID-CPA *secure in* $\mathcal{G}$ *under the* $\mathcal{D}_k$-MDDH *assumption for* $\mathbb{G}_1$ *if* MAC *is* HPR_0-CMA *secure in* $\mathbb{G}_2$. *Precisely, for all adversaries* $\mathcal{A}$ *there exists adversaries* $\mathcal{B}_1$ *and* $\mathcal{B}_2$ *with*

$$\mathsf{Adv}^{\mathsf{ind\text{-}hid\text{-}cpa}}_{\mathsf{HIBKEM}[\mathsf{MAC},\mathcal{D}_k],\mathcal{G}}(\mathcal{A}) \leq \mathsf{Adv}^{\mathsf{hpr_0\text{-}cma}}_{\mathsf{MAC},\mathbb{G}_2}(\mathcal{B}_1) + \mathsf{Adv}^{\mathsf{mddh}}_{\mathcal{D}_k,\mathsf{GGen},\mathbb{G}_1}(\mathcal{B}_2)$$

and $T(\mathcal{B}_1) + T(\mathcal{B}_2) \approx T(\mathcal{A}) + Q \cdot \mathsf{poly}(\lambda)$.

The detailed proof of Theorem 3 can be found in full version.

4.1 Instantiations

MDDH. The result of applying the HIBKEM transformation to $\mathsf{MAC}_1[\mathcal{U}_{3k,k}]$ is shown in Fig. 11. The scheme has $\alpha\left(L^2+L\right)\left(4k^2+k\right)+3k^2+2k$ group elements in the public key and $4k+1$ group elements in the ciphertext. The user secret keys have at most $\alpha\left(L^2/2+L/2-1\right)(k+1)+4k+1$ group elements. Identities that are deeper in the hierarchy have smaller secret keys, since the user secret key size is dominated by the size of the delegation keys. On the last level, the user secret keys consist of only $4k+1$ keys.

The result of applying the HIBKEM transformation to $\mathsf{MAC}_2[\mathcal{U}_{3k,k}]$ is shown in Fig. 12. The scheme has $\alpha\left(L^2+L\right)\left(4k^2+k\right)+3k^2+2k$ group elements in the public key and $3Lk+k+1$ group elements in the ciphertext. The user secret keys have at most $3Lk+k+1$ group elements. Identities that are deeper in the hierarchy have larger secret keys.

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

SXDH. With a type III pairing, both of our schemes can be instantiated with the SXDH assumption. The results can be found in the full version.

```
$\underline{\mathsf{Gen}(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e):}$
$\mathsf{sk}_{\mathsf{MAC}} \xleftarrow{\$} \mathsf{Gen}_{\mathsf{MAC}}(\mathbb{G}_2, q, P_2)$
$\textbf{Parse } \mathsf{sk}_{\mathsf{MAC}} =: (\mathbf{B}, \widetilde{\mathbf{x}}, x_0')$
$\textbf{Parse } \widetilde{\mathbf{x}} =: (\mathbf{x}_{l,i,j})_{1 \le l \le \ell(L), 1 \le i \le L, 1 \le j \le \ell'(l,i)}$
$\mathbf{A} \xleftarrow{\$} \mathcal{D}_k$
$\textbf{for } l \in \{1, \dots, \ell(L)\}, i \in \{1, \dots, L\}, j \in \{1, \dots, \ell'(l,i)\} \textbf{ do}$
    $\mathbf{Y}_{l,i,j} \xleftarrow{\$} \mathbb{Z}_q^{k \times n}$; $\mathbf{Z}_{l,i,j} := \left(\mathbf{Y}_{l,i,j}^\top \mid \mathbf{x}_{l,i,j}\right) \cdot \mathbf{A}$
    $\mathbf{d}_{l,i,j} := \mathbf{x}_{l,i,j}^\top \cdot \mathbf{B}$; $\mathbf{E}_{l,i,j} := \mathbf{Y}_{l,i,j} \cdot \mathbf{B}$
$\mathbf{y}_0' \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{z}_0' := \left(\mathbf{y}_0'^\top \mid x_0'\right) \cdot \mathbf{A}$
$\widetilde{\mathbf{Z}} := \left([\mathbf{Z}_{l,i,j}]_1\right)_{1 \le l \le \ell(L), 1 \le i \le L, 1 \le j \le \ell'(l,i)}$
$\mathsf{pk} := \left(\mathcal{G}, [\mathbf{A}]_1, \widetilde{\mathbf{Z}}, [\mathbf{z}_0']_1\right)$
$\widetilde{\mathsf{dk}} := \left([\mathbf{d}_{l,i,j}]_2, [\mathbf{E}_{l,i,j}]_2\right)_{1 \le l \le \ell(L), 1 \le i \le L, 1 \le j \le \ell'(l,i)}$
$\mathsf{dk} := \left([\mathbf{B}]_2, \widetilde{\mathsf{dk}}\right)$
$\mathsf{sk} := \left(\mathsf{sk}_{\mathsf{MAC}}, (\mathbf{Y}_{l,i,j})_{1 \le l \le \ell(p), 1 \le i \le L, 1 \le j \le \ell'(l,i)}, , \mathbf{y}_0'\right)$
$\textbf{return } (\mathsf{pk}, \mathsf{dk}, \mathsf{sk})$
```

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

```
$\underline{\mathsf{Ext}(\mathsf{sk}, \mathsf{id} \in \mathcal{S}^p):}$
$\left(\left([\mathbf{t}_l]_2\right)_{1 \le l \le \ell(p)}, [u]_2\right) \xleftarrow{\$} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{id})$
$\mathbf{v} := \sum_{l=1}^{\ell(p)} \left(\sum_{i=1}^{p} \sum_{j=1}^{\ell'(l,i)} f_{l,i,j}\left(\mathsf{m}_{|i}\right)\mathbf{Y}_{l,i,j}\right)\mathbf{t}_l + \mathbf{y}_0'$
$\textbf{for } l \in \{1, \dots, \ell(p)\}, i \in \{p+1, \dots, L\}, j \in \{1, \dots, \ell'(l,i)\} \textbf{ do}$
    $d_{l,i,j} := \mathbf{x}_{l,i,j}^\top \mathbf{t}_l$
    $\mathbf{e}_{l,i,j} := \mathbf{Y}_{l,i,j}\mathbf{t}_l$
$\mathsf{usk} := \left(\left([\mathbf{t}_l]_2\right)_{1 \le l \le \ell(p)}, [u]_2, [\mathbf{v}]_2\right)$
$\mathsf{udk} := \left([d_{l,i,j}]_2, [\mathbf{e}_{l,i,j}]_2\right)_{1 \le l \le \ell(p), 1 \le i \le L, 1 \le j \le \ell'(l,i)}$
$\textbf{return } (\mathsf{usk}, \mathsf{udk})$
```

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

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

Fig. 10. The transformation of an affine MAC with levels to a HIBKEM.

```
$\mathsf{Gen}(1^\lambda)$:
$\mathbf{B} \overset{\$}{\leftarrow} \mathcal{U}_{3k,k}$; $\mathbf{A} \overset{\$}{\leftarrow} \mathcal{D}_k$
for $i \in \{1, \dots, L\}, j \in \{1, \dots, i\alpha\}, b \in \{0,1\}$ do
    $\mathbf{x}_{i,j,b} \overset{\$}{\leftarrow} \mathbb{Z}_q^{3k}$ $\mathbf{Y}_{i,j,b} \overset{\$}{\leftarrow} \mathbb{Z}_q^{k \times n}$
    $\mathbf{Z}_{i,j,b} := \left(\mathbf{Y}_{i,j,b}^\top \mid \mathbf{x}_{i,j,b}\right) \cdot \mathbf{A}$
    $\mathbf{d}_{i,j,b} := \mathbf{x}_{i,j,b}^\top \mathbf{B}$; $\mathbf{E}_{i,j,b} := \mathbf{Y}_{i,j,b} \mathbf{B}$
$x'_0 \overset{\$}{\leftarrow} \mathbb{Z}_q$; $\mathbf{y}'_0 \overset{\$}{\leftarrow} \mathbb{Z}_q^k$; $\mathbf{z}'_0 := \left(\mathbf{y}_0'^\top \mid x'_0\right) \cdot \mathbf{A}$
$\widetilde{\mathbf{Z}} := \left([\mathbf{Z}_{i,j,b}]_1\right)_{1 \le i \le L, b \in \{0,1\}, 1 \le j \le i\alpha}$
$\mathsf{pk} := \left(\mathcal{G}, [\mathbf{A}]_1, \widetilde{\mathbf{Z}}, [\mathbf{z}'_0]_1\right)$
$\widetilde{\mathsf{dk}} := \left([\mathbf{d}_{i,j,b}]_2, [\mathbf{E}_{i,j,b}]_2\right)_{1 \le i \le L, b \in \{0,1\}, 1 \le j \le i\alpha}$
$\mathsf{dk} := \left([\mathbf{B}]_2, \widetilde{\mathsf{dk}}\right)$
$\widetilde{\mathbf{Y}} := (\mathbf{Y}_{i,j,b})_{1 \le i \le L, b \in \{0,1\}, 1 \le j \le i\alpha}$
$\mathsf{sk} := \left(\mathsf{sk}_{\mathsf{MAC}}, \widetilde{\mathbf{Y}}, \mathbf{y}'_0\right)$
return $(\mathsf{pk}, \mathsf{dk}, \mathsf{sk})$
```

```
$\mathsf{Ext}(\mathsf{sk}, \mathsf{id} \in \mathcal{S}^p)$:
$\mathbf{s} \overset{\$}{\leftarrow} \mathbb{Z}_q^k$; $\mathbf{t} := \mathbf{B}\mathbf{s}$
$u := \left(\sum_{i=1}^{p} \sum_{j=1}^{i\alpha} \mathbf{x}_{i,j,[\![\mathsf{id}]\!]_j}^\top\right)\mathbf{t} + x'_0$
$\mathbf{v} := \left(\sum_{i=1}^{p} \sum_{j=1}^{i\alpha} \mathbf{Y}_{i,j,[\![\mathsf{id}]\!]_j}\right)\mathbf{t} + \mathbf{y}'_0$
for $i \in \{p+1, \dots, L\}, j \in \{1, \dots, i\alpha\}, b \in \{0,1\}$ do
    $d_{i,j,b} := \mathbf{x}_{i,j,b}^\top \mathbf{t}$; $\mathbf{e}_{i,j,b} := \mathbf{Y}_{i,j,b}^\top \mathbf{t}$
$\mathsf{usk} := \left([\mathbf{t}]_2, [u]_2, [\mathbf{v}]_2\right)$
$\mathsf{udk} := \left([d_{i,j,b}]_2, [\mathbf{e}_{i,j,b}]_2\right)_{p+1 \le i \le L, b \in \{0,1\}, 1 \le j \le i\alpha}$
return $(\mathsf{usk}, \mathsf{udk})$
```

```
$\mathsf{Del}(\mathsf{dk}, \mathsf{usk}, \mathsf{udk}, \mathsf{id} \in \mathcal{S}^p, \mathsf{id}_{p+1} \in \mathcal{S})$:
Parse $\mathsf{usk} =: \left([\mathbf{t}]_2, [u]_2, [\mathbf{v}]_2\right)$
$\mathbf{s}' \overset{\$}{\leftarrow} \mathbb{Z}_q^{n'}$; $\mathbf{t}' := \mathbf{t} + \mathbf{B}\mathbf{s}'$
$u' := u + \left(\sum_{i=1}^{p+1} \sum_{j=1}^{i\alpha} \mathbf{d}_{i,j,[\![\mathsf{id}]\!]_j}\right)\mathbf{s}'$
$\mathbf{v}' := \mathbf{v} + \left(\sum_{i=1}^{p+1} \sum_{j=1}^{\ell'(l,i)} \mathbf{E}_{i,j,[\![\mathsf{id}]\!]_j}\right)\mathbf{s}'$
for $i \in \{p+1, \dots, L\}, j \in \{1, \dots, i\alpha\}, b \in \{0,1\}$ do
    $d'_{i,j,b} := d_{i,j,b} + \mathbf{d}_{i,j,b}\mathbf{s}'$
    $\mathbf{e}'_{i,j,b} := \mathbf{e}_{i,j,b} + \mathbf{E}_{i,j,b}\mathbf{s}'$
$\mathsf{usk}' := \left([\mathbf{t}']_2, [u']_2, [\mathbf{v}']_2\right)$
$\mathsf{udk}' := \left(\left[d'_{i,j,b}\right]_2, \left[\mathbf{e}'_{i,j,b}\right]_2\right)_{p+2 \le i \le L, 1 \le j \le i\alpha, b \in \{0,1\}}$
return $(\mathsf{usk}', \mathsf{udk}')$
```

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

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

Fig. 11. The resulting scheme $\mathsf{HIBKEM}\left[\mathsf{MAC}_1[\mathcal{U}_{3k,k}], \mathcal{D}_k\right]$.

```
$\underline{\mathsf{Gen}(1^\lambda)}$:
$\mathbf{B} \xleftarrow{\$} \mathcal{U}_{3k,k}$; $\mathbf{A} \xleftarrow{\$} \mathcal{D}_k$
for $i \in \{1,\dots,L\}, j \in \{1,\dots,i\alpha\}, b \in \{0,1\}$ do
    $\mathbf{x}_{i,j,b} \xleftarrow{\$} \mathbb{Z}_q^{3k}$ $\mathbf{Y}_{i,j,b} \xleftarrow{\$} \mathbb{Z}_q^{k \times n}$
    $\mathbf{Z}_{i,j,b} := \left(\mathbf{Y}_{i,j,b}^\top \mid \mathbf{x}_{i,j,b}\right) \cdot \mathbf{A}$
    $\mathbf{d}_{i,j,b} := \mathbf{x}_{i,j,b}^\top \mathbf{B}$; $\mathbf{E}_{i,j,b} := \mathbf{Y}_{i,j,b}\mathbf{B}$
$x'_0 \xleftarrow{\$} \mathbb{Z}_q$; $\mathbf{y}'_0 \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{z}'_0 := \left(\mathbf{y}_0'^\top \mid x'_0\right) \cdot \mathbf{A}$
$\widetilde{\mathbf{Z}} := \left([\mathbf{Z}_{i,j,b}]_1\right)_{1 \le i \le L, b \in \{0,1\}, 1 \le j \le i\alpha}$
$\mathsf{pk} := \left(\mathcal{G}, [\mathbf{A}]_1, \widetilde{\mathbf{Z}}, [\mathbf{z}'_0]_1\right)$
$\widetilde{\mathsf{dk}} := \left([\mathbf{d}_{i,j,b}]_2, [\mathbf{E}_{i,j,b}]_2\right)_{\substack{1 \le i \le L, b \in \{0,1\}, \\ 1 \le j \le i\alpha}}$
$\mathsf{dk} := \left([\mathbf{B}]_2, \widetilde{\mathsf{dk}}\right)$
$\widetilde{\mathbf{Y}} := (\mathbf{Y}_{i,j,b})_{1 \le i \le L, b \in \{0,1\}, 1 \le j \le i\alpha}$
$\mathsf{sk} := \left(\mathsf{sk}_{\mathsf{MAC}}, \widetilde{\mathbf{Y}}, \mathbf{y}'_0\right)$
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 $\mathbf{s}_i \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{t}_i := \mathbf{B}\mathbf{s}_i$
$u := \sum_{i=1}^{p} \left(\sum_{j=1}^{i\alpha} \mathbf{x}_{i,j,[\![\mathsf{id}]\!]_j}^\top\right)\mathbf{t}_i + x'_0$
$\mathbf{v} := \sum_{i=1}^{p} \left(\sum_{j=1}^{i\alpha} \mathbf{Y}_{i,j,[\![\mathsf{id}]\!]_j}\right)\mathbf{t}_i + \mathbf{y}'_0$
return $\left(\left([\mathbf{t}_i]_2\right)_{1 \le i \le p}, [u]_2, [\mathbf{v}]_2\right)$
```

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

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

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

Fig. 12. The resulting scheme $\mathsf{HIBKEM}\left[\mathsf{MAC}_2[\mathcal{U}_{3k,k}], \mathcal{D}_k\right]$.

References

1. Abe, M., Hofheinz, D., Nishimaki, R., Ohkubo, M., Pan, J.: Compact structure-preserving signatures with almost tight security. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017. LNCS, vol. 10402, pp. 548–580. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-63715-0_19
2. Bader, C., Hofheinz, D., Jager, T., Kiltz, E., Li, Y.: Tightly-secure authenticated key exchange. In: Dodis, Y., Nielsen, J.B. (eds.) TCC 2015. LNCS, vol. 9014, pp. 629–658. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46494-6_26
3. Blazy, O., Kiltz, E., Pan, J.: (Hierarchical) identity-based encryption from affine message authentication. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014. LNCS, vol. 8616, pp. 408–425. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-44371-2_23
4. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44647-8_13

5. Canetti, R., Halevi, S., Katz, J.: Chosen-ciphertext security from identity-based encryption. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 207–222. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24676-3_13
6. Chen, J., Gay, R., Wee, H.: Improved dual system ABE in prime-order groups via predicate encodings. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9057, pp. 595–624. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46803-6_20
7. Chen, J., Lim, H.W., Ling, S., Wang, H., Wee, H.: Shorter IBE and signatures via asymmetric pairings. In: Abdalla, M., Lange, T. (eds.) Pairing 2012. LNCS, vol. 7708, pp. 122–140. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-36334-4_8
8. Chen, J., Wee, H.: Fully, (Almost) tightly secure IBE and dual system groups. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8043, pp. 435–460. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40084-1_25
9. Cocks, C.: An identity based encryption scheme based on quadratic residues. In: Honary, B. (ed.) Cryptography and Coding 2001. LNCS, vol. 2260, pp. 360–363. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45325-3_32
10. Escala, A., Herold, G., Kiltz, E., Ràfols, C., Villar, J.: An algebraic framework for Diffie-Hellman assumptions. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8043, pp. 129–147. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40084-1_8
11. Gay, R., Hofheinz, D., Kiltz, E., Wee, H.: Tightly CCA-secure encryption without pairings. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016. LNCS, vol. 9665, pp. 1–27. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49890-3_1
12. Gay, R., Hofheinz, D., Kohl, L., Pan, J.: More efficient (almost) tightly secure structure-preserving signatures. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018. LNCS, vol. 10821, pp. 230–258. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-78375-8_8
13. Gentry, C.: Practical identity-based encryption without random oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445–464. Springer, Heidelberg (2006). https://doi.org/10.1007/11761679_27
14. Gentry, C., Silverberg, A.: Hierarchical ID-based cryptography. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 548–566. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-36178-2_34
15. Gong, J., Cao, Z., Tang, S., Chen, J.: Extended dual system group and shorter unbounded hierarchical identity based encryption. Des. Codes Crypt. **80**(3), 525–559 (2016). https://doi.org/10.1007/s10623-015-0117-z
16. 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.) ASIACRYPT 2016. LNCS, vol. 10032, pp. 624–654. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53890-6_21
17. Hesse, J., Hofheinz, D., Kohl, L.: On tightly secure non-interactive key exchange. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018, Part II. LNCS, vol. 10992, pp. 65–94. Springer, Heidelberg (Aug (2018)
18. Hofheinz, D., Jager, T.: Tightly secure signatures and public-key encryption. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 590–607. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32009-5_35

19. Hofheinz, D., Jia, D., Pan, J.: Identity-based encryption tightly secure under chosen-ciphertext attacks. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018. LNCS, vol. 11273, pp. 190–220. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-03329-3_7
20. Hofheinz, D., Kiltz, E.: Secure hybrid encryption from weakened key encapsulation. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 553–571. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74143-5_31
21. 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. LNCS, vol. 9020, pp. 799–822. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46447-2_36
22. Horwitz, J., Lynn, B.: Toward hierarchical identity-based encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 466–481. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-46035-7_31
23. Jutla, C.S., Roy, A.: Shorter quasi-adaptive NIZK proofs for linear subspaces. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013. LNCS, vol. 8269, pp. 1–20. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-42033-7_1
24. Kiltz, E., Neven, G.: Identity-based signatures. In: Joye, M., Neven, G. (eds.) Identity-Based Cryptography. IOS Press, Amsterdam (2009)
25. Kiltz, E., Pan, J., Wee, H.: Structure-preserving signatures from standard assumptions, revisited. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9216, pp. 275–295. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48000-7_14
26. Kiltz, E., Wee, H.: Quasi-adaptive NIZK for linear subspaces revisited. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9057, pp. 101–128. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46803-6_4
27. Lewko, A.: Tools for simulating features of composite order bilinear groups in the prime order setting. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 318–335. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_20
28. Lewko, A., Waters, B.: Why proving HIBE systems secure is difficult. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 58–76. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55220-5_4
29. Naor, M., Reingold, O.: On the construction of pseudo-random permutations: Luby-Rackoff revisited (extended abstract). In: 29th ACM STOC, pp. 189–199. ACM Press, May 1997
30. Sakai, R., Ohgishi, K., Kasahara, M.: Cryptosystems based on pairing. In: SCIS 2000, Okinawa, Japan, January 2000
31. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985). https://doi.org/10.1007/3-540-39568-7_5
32. Waters, B.: Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 619–636. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03356-8_36
33. Waters, B.: Efficient identity-based encryption without random oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005). https://doi.org/10.1007/11426639_7
34. Wee, H.: Dual system encryption via predicate encodings. In: Lindell, Y. (ed.) TCC 2014. LNCS, vol. 8349, pp. 616–637. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-54242-8_26