# Hierarchical Identity-Based Encryption with Tight Multi-Challenge Security

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

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

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

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

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

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

## 1 Introduction

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

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

We consider a reduction *tight* if $\ell$ is a small constant and the running time of $\mathcal{B}$ is approximately the same as that of $\mathcal{A}$. Many existing works [8,11,12,13] consider a notion of tightness called "almost tight security". Different to the (full) tightness, almost tight security allows the security loss $\ell$ to be a small polynomial, which is usually a linear function of the security parameter, but still independent of the size of $\mathcal{A}$. We do not distinguish these two notions, but we are precise about the security loss in our comparison tables and security proofs.

Tight reductions are not only theoretically interesting but also beneficial in practice. A tight reduction enables us to give universal key-length recommendations that are independent of the size of an application and shorter than the non-tight ones. This is, in particular, useful in the setting where the envisioned size of an application cannot be reasonably bounded a priori. As a result of that, many recent works have been pursuing efficient tightly secure cryptographic schemes, including digital signature [21,26,13], public-key encryption [11,20,12], identity-based encryption [8,5] schemes, and authenticated key exchange protocols [15].

HIBE meets Tight Security. In this paper, we focus on hierarchical identity-based encryption (HIBE) schemes [24,14]. In an $L$-level HIBE, an identity is a vector of maximal $L$ identities. It is considered to be more difficult to construct HIBE than IBE and PKE since an HIBE scheme provides more functionalities. For instance, an $L$-level HIBE scheme allows a user at level $\alpha < L$ to delegate a secret key for its descendants at level $\alpha' > \alpha$.

Constructing tightly secure HIBE appears to be much more challenging. The first tightly secure IBE from standard assumptions was constructed in 2013 [8], while the first tightly secure HIBE was just proposed very recently [28]. We believe that it is not a coincidence. Firstly, Lewko and Waters [32] showed the potential difficulty of constructing tightly secure HIBE. More precisely, they proved that there is a (relatively) large class of HIBE schemes that cannot be tightly proven secure. Secondly, Blazy, Kiltz, and Pan (BKP) [5] made the first attempt to bypass the aforementioned impossibility result. Unfortunately, it has been found that the BKP proof strategy is insufficient for the tight adaptive security of HIBE (cf. [6] and Appendix A of [29]). Adaptive security allows an adversary $\mathcal{A}$ to adaptively choose a challenge identity $\mathsf{id}^\star$ after it sees the master public key and asks for polynomial many user secret keys for identities chosen by $\mathcal{A}$.

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

From Single- to Multi-Challenge Security. In the real world, an adversary can learn ciphertexts of multiple challenge identities. This is captured by the more realistic multi-challenge security. We note that single-challenge security implies multi-challenge security via a straightforward, but non-tight reduction. This is mainly the reason why the security of many (H)IBE schemes (e.g. [35,31,30,5,28]) is analyzed in this simple single-challenge setting. However, this straightforward "single- to multi-challenge" reduction loses a relatively large polynomial factor. Namely, if an adversary makes $Q_c$ many queries for challenge ciphertexts, then the overall security loses a factor of $Q_c$. This defeats the purpose of establishing tight reductions for the overall scheme in a more realistic setting.

Our Goal: HIBE with Tight Multi-Challenge Security. We aim at constructing tightly secure HIBE schemes in the more realistic multi-challenge setting. We note that there exist several techniques in constructing tightly multi-challenge secure IBE schemes (for instance, [23,17,18,22]) in composite- or prime-order pairing groups. However, as already observed by the LP paper, these techniques cannot be easily used in the HIBE setting. Thus, to achieve our goal, it requires us to develop a new technique for tight multi-challenge security that is useful for HIBE schemes.

### 1.1 Our Contribution

We construct the *first* tightly chosen-plaintext secure HIBE schemes in the multi-challenge setting. The main novelty of this paper is a new randomization technique that enables us to randomize user secret keys for hierarchical identities in the multi-challenge setting. We highlight that our technique improves the existing techniques [23,17,18,22] for tightly multi-challenge secure IBE schemes in the sense that ours can handle randomization for identities with flexible lengths. We postpone the detailed comparison of these techniques in Section 1.3.

Following the "MAC-to-(H)IBE" framework [5,28], we capture our core technique with the notion of affine MACs with levels (which was firstly proposed in [28]) in the multi-challenge setting. By using prime-order pairings and the Matrix Decisional Diffie-Hellman (MDDH) assumption [10], we compile any of these MAC schemes to an HIBE tightly in the multi-challenge setting. We have two main constructions of the affine MACs, $\mathsf{MAC}_1$ and $\mathsf{MAC}_2$, and they give us two HIBE with different advantages and disadvantages, respectively: Considering identity space $\mathcal{ID} := (\{0,1\}^n)^{\leq L}$, our first scheme has constant amount of group elements in the ciphertext, but $\mathbf{O}(nL)$ many elements in the user secret key; and our second scheme has shorter user secret key that contains $\mathbf{O}(L)$ many elements, but its ciphertext contains $\mathbf{O}(L)$ many elements. Both schemes have security loss $\mathbf{O}(n \cdot L^2)$ and independent of the numbers of challenge ciphertext queries and user secret key queries. Table 1 compares our schemes with the existing HIBE schemes in prime-order pairing groups.

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

Anonymity. Additionally, the first construction of our MACs, $\mathsf{MAC}_1$, has tight anonymity. By using the anonymity-preserving transformation of [5], we construct the *first* tightly secure, anonymous HIBE scheme in the multi-challenge setting. An (H)IBE scheme is anonymous if its challenge ciphertexts hide the corresponding identities. An application of anonymous HIBE is PKE with keyword search [1].

| Scheme | $\lvert\mathsf{mpk}\rvert$ | $\lvert\mathsf{usk}\rvert$ | $\lvert\mathsf{C}\rvert$ | Loss | MC | Ass. |
|---|---|---|---|---|---|---|
| Wat05 [35] | $\mathbf{O}(nL)\lvert\mathbb{G}\rvert$ | $\mathbf{O}(nL)\lvert\mathbb{G}\rvert$ | $(1+p)\lvert\mathbb{G}\rvert$ | $\mathbf{O}(nQ_{\mathsf{e}})^L$ | ✗ | DBDH |
| Wat09 [34] | $\mathbf{O}(L)\lvert\mathbb{G}\rvert$ | $\mathbf{O}(p)(\lvert\mathbb{G}\rvert+\lvert\mathbb{Z}_q\rvert)$ | $\mathbf{O}(p)(\lvert\mathbb{G}\rvert+\lvert\mathbb{Z}_q\rvert)$ | $\mathbf{O}(Q_{\mathsf{e}})$ | ✗ | 2-LIN |
| Lew12 [30] | $60\lvert\mathbb{G}\rvert+2\lvert\mathbb{G}_T\rvert$ | $(60+10p)\lvert\mathbb{G}\rvert$ | $10p\lvert\mathbb{G}\rvert$ | $\mathbf{O}(Q_{\mathsf{e}}L)$ | ✗ | 2-LIN |
| CW13 [8] | $\mathbf{O}(Lk^2)(\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert)$ | $\mathbf{O}(Lk)\lvert\mathbb{G}_2\rvert$ | $(2k+2)\lvert\mathbb{G}_1\rvert$ | $\mathbf{O}(Q_{\mathsf{e}})$ | ✗ | $k$-LIN |
| BKP14 [5] | $\mathbf{O}(Lk^2)(\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert)$ | $\mathbf{O}(Lk)\lvert\mathbb{G}_2\rvert$ | $(2k+2)\lvert\mathbb{G}_1\rvert$ | $\mathbf{O}(Q_{\mathsf{e}})$ | ✗ | $k$-LIN |
| GCTC16 [16] | $(6k^2+12k)(\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert)$ $+(k+2)\lvert\mathbb{G}_T\rvert$ | $((6k+12)\lceil p/3\rceil$ $-(k+2)p)\lvert\mathbb{G}_2\rvert$ | $(3k+6)\lceil p/3\rceil\lvert\mathbb{G}_1\rvert$ | $\mathbf{O}(QL)$ | ✗ | $k$-LIN |
| $\mathsf{LP19}_1$ [28] | $\mathbf{O}(nL^2k^2)(\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert)$ | $\mathbf{O}(nL^2k)\lvert\mathbb{G}_2\rvert$ | $(4k+1)\lvert\mathbb{G}_1\rvert$ | $\mathbf{O}(nL^2k)$ | ✗ | $k$-LIN |
| $\mathsf{LP19}_1^{\mathcal{H}}$ [28] | $\mathbf{O}(\gamma Lk^2)(\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert)$ | $\mathbf{O}(\gamma Lk)\lvert\mathbb{G}_2\rvert$ | $(4k+1)\lvert\mathbb{G}_1\rvert$ | $\mathbf{O}(\gamma Lk)$ | ✗ | $k$-LIN |
| $\mathsf{LP19}_2$ [28] | $\mathbf{O}(nL^2k^2)(\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert)$ | $(3kp+k+1)\lvert\mathbb{G}_2\rvert$ | $(3kp+k+1)\lvert\mathbb{G}_1\rvert$ | $\mathbf{O}(nLk)$ | ✗ | $k$-LIN |
| $\mathsf{LP19}_2^{\mathcal{H}}$ [28] | $\mathbf{O}(\gamma Lk^2)(\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert)$ | $(3kp+k+1)\lvert\mathbb{G}_2\rvert$ | $(3kp+k+1)\lvert\mathbb{G}_1\rvert$ | $\mathbf{O}(\gamma k)$ | ✗ | $k$-LIN |
| $\mathsf{HIBKEM}_1$ | $\mathbf{O}(nL^2k^2)(\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert)$ | $\mathbf{O}(nL^2k)\lvert\mathbb{G}_2\rvert$ | $5k\lvert\mathbb{G}_1\rvert$ | $\mathbf{O}(nL^2k)$ | ✓ | $k$-LIN |
| $\mathsf{HIBKEM}_1^{\mathcal{H}}$ | $\mathbf{O}(\gamma Lk^2)(\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert)$ | $\mathbf{O}(\gamma Lk)\lvert\mathbb{G}_2\rvert$ | $5k\lvert\mathbb{G}_1\rvert$ | $\mathbf{O}(\gamma Lk)$ | ✓ | $k$-LIN |
| $\mathsf{HIBKEM}_2$ | $\mathbf{O}(nL^2k^2)(\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert)$ | $(3kp+2k)\lvert\mathbb{G}_2\rvert$ | $(3kp+2k)\lvert\mathbb{G}_1\rvert$ | $\mathbf{O}(nLk)$ | ✓ | $k$-LIN |
| $\mathsf{HIBKEM}_2^{\mathcal{H}}$ | $\mathbf{O}(\gamma Lk^2)(\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert)$ | $(3kp+2k)\lvert\mathbb{G}_2\rvert$ | $(3kp+2k)\lvert\mathbb{G}_1\rvert$ | $\mathbf{O}(\gamma k)$ | ✓ | $k$-LIN |

**Table 1.** Comparison of HIBEs in prime-order pairing groups with adaptive security in the standard model based on static assumptions. The highlighted rows are from this paper. The schemes with $\mathcal{H}$ in the superscript are obtained by hashing the identities as described in the full version of [28].

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

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

Chosen-Ciphertext Security. We note that ciphertexts of our HIBE schemes have compatible structure to use Quasi-Adaptive Non-Interactive Zero-Knowledge (QANIZK) argument for linear subspace systems [25,27,22,2]. Similar to [22], we upgrade our schemes to chosen-ciphertext security by using any tightly unbounded simulation-sound QANIZK scheme. These schemes are the first tightly chosen-ciphertext secure HIBE schemes in the multi-challenge setting. Combining with the technique in the first extension, we also construct a tightly chosen-ciphertext secure and anonymous HIBE.

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

In the full version of [28], they use a collision-resistant hash function to further improve the security loss and master public key size of their schemes. Here we can also do the same improvement.

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

### 1.2 Technical Details

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

Starting Point: The BKP Framework. To set up the stage of our discussion, we recall the BKP framework [5], which transforms an algebraic MAC scheme to an IBE scheme in prime-order pairing groups. The algebraic MAC is called affine MAC, due to its affine structure. Their framework is an abstraction of the Chen-Wee (CW) IBE [8] and can also be viewed as an extension of the "MAC-to-Signature" framework by Bellare and Goldwasser (BG) [4] in the IBE context. In particular, the BKP framework can be viewed as a fine-grained reverse of the Naor transformation [7] on the BG signature scheme.

We give some informal ideas about how an affine MAC can be turned into an IBE. The master public key of an IBE, $\mathsf{pk} := \mathsf{Com}(\mathsf{sk}_{\mathsf{MAC}})$, is a commitment of the MAC secret key, $\mathsf{sk}_{\mathsf{MAC}}$. A user secret key $\mathsf{usk}[\mathsf{id}]$ of an identity $\mathsf{id}$ consists of a BG signature, namely, a MAC tag $\tau_{\mathsf{id}}$ on the message $\mathsf{id}$ and a NIZK proof of the validity of $\tau_{\mathsf{id}}$ w.r.t. the secret key committed in $\mathsf{pk}$. The observation of BKP is that one can implement these commitments and NIZK proofs with the (tuned) Groth-Sahai proof system [19].

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

Obstacles in Achieving our Goal with BKP. The BKP framework has a nice property that the security of the IBE scheme can be tightly reduced to the security of the MAC scheme. Thus, we can only focus on constructing tightly secure MAC, which is more fundamental. In particular, the BKP framework has a tightly secure MAC scheme $\mathsf{MAC}_{\mathsf{NR}}$ in the single-challenge setting under a standard assumption. $\mathsf{MAC}_{\mathsf{NR}}$ is implicitly in the CW IBE and borrows some idea from the Naor-Reingold PRF [33]. However, $\mathsf{MAC}_{\mathsf{NR}}$ has limitations that

(a) it can only be used to handle at most one IBE challenge ciphertext, and

(b) it cannot provide tight adaptive security for HIBE.

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

Let $\mathbb{G}_2 := \langle P_2 \rangle$ be an additive prime-order group. We use the implicit notation $[x]_2 := xP_2$ as in [10]. $\mathsf{MAC}_{\mathsf{NR}}$ chooses $\mathbf{B} \in \mathbb{Z}_q^{(k+1)\times k}$ according to the underlying assumption. $\mathbf{B}$ always has rank $k$ and, for simplicity, we assume that the first $k$ rows of $\mathbf{B}$, denoted by $\overline{\mathbf{B}}$, forms a full-rank square matrix. For message space $\mathcal{M} := \{0,1\}^n$, which is the same as the identity space of the resulting IBE, its secret key is chosen uniformly at random and has the form of

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

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

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

Based on the MDDH assumption, $\mathsf{MAC}_{\mathsf{NR}}$ is tightly pseudorandom against chosen-message attacks ($\mathsf{PR\text{-}CMA}$ security), which is a decisional variant of the standard existential unforgeability against chosen-message attacks ($\mathsf{EUF\text{-}CMA}$ security) for MAC schemes [9]. Essentially, the $\mathsf{PR\text{-}CMA}$ security of $\mathsf{MAC}_{\mathsf{NR}}$ shows that $[u]_2$ is pseudorandom.

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

The overall proof strategy of $\mathsf{MAC}_{\mathsf{NR}}$ is to gradually randomize all the $u$ values in answering $\mathcal{A}$'s tag queries. During this process, the reduction must be able to compute $u^\star = \sum_i \mathbf{x}_{i,\mathsf{m}_i^\star}^\top \mathbf{t}^\star + x_0'$ for a fresh $\mathsf{m}^\star$, which is the main difficulty in the proof. To solve it, the BKP argument conceptually replace $x_0'$ with a constant random function $\mathsf{RF}_0(\varepsilon)$. Then, by using the MDDH assumption, it develops a random function $\mathsf{RF}_{i+1} : \{0,1\}^{i+1} \to \mathbb{Z}_q$ from another random function $\mathsf{RF}_i : \{0,1\}^i \to \mathbb{Z}_q$ on-the-fly for some integer $0 \le i < n$. After $n$ recursions, a random function $\mathsf{RF} : \{0,1\}^n \to \mathbb{Z}_q$ is developed and thus the security loss of $\mathsf{MAC}_{\mathsf{NR}}$ is $\mathbf{O}(n)$. More precisely, in each step, the reduction guesses the $(i+1)$-th bit of $\mathsf{m}^\star$ as $b^\star \in \{0,1\}$ and defines the function $\mathsf{RF}_{i+1}$ as:

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

where $\mathsf{m}_{|i}$ is the first $i$ bits of $\mathsf{m}$ and $R_{\mathsf{m}_{|i}}$ is a random value from $\mathbb{Z}_q$ chosen for $\mathsf{m}_{|i}$. Alternatively, the BKP strategy can be viewed as gradually injecting randomness directly into $x_0'$, during developing the random function above.

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

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

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

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

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

Step 1: New Strategy for Tight Multi-Challenge Security. We call this randomization strategy subspace randomization, since it first increases the dimension of $\mathbf{t}$ in the tag so that there exist subspaces, and our crucial randomization happens in some of these subspaces. This subspace randomization is compatible with the independent randomization of Langrehr and Pan [28] and, thus, it gets extended in Step 2 to randomize MAC tags for messages with flexible length, namely, hierarchical identities.

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

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

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

Namely,

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

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

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

More precisely, in our Hybrid $i$, for a tag query on $\mathsf{m}$, our $u_\mathsf{m}$ has the form

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

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

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

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

Now we can introduce $\mathsf{RF}_{i+1}$ and, after $n$ of these recursions, we can have $\mathsf{RF}_n$ to randomize all the tags.

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

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

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

We are not claiming any efficiency improvement with this IBE, but technical achievement, instead, since it has roughly the same efficiency as its counterparts from [17,18,22]. However, our techniques involved in this IBE scheme improves those in [17,18,22] in the sense that ours can be extended to randomize user secret keys for hierarchical identities, while those in [17,18,22] cannot.

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

The strategy in this step is motivated by the work of Langrehr and Pan [28], where their core technique is to isolate the randomization for messages at different levels (which will be identities at different levels in the HIBE). To implement this, we add a "layer" to $\mathbf{t}$ by choosing $\mathbf{t}$ from $\mathbb{Z}_q^{3k}$. Similar to Step 1, we exploit some properties of the linear space $\mathbb{Z}_q^{3k}$. We choose two random matrices $\mathbf{B}_0, \mathbf{B}_1 \overset{\$}{\leftarrow} \mathbb{Z}_q^{3k \times k}$ and decompose $\mathbb{Z}_q^{3k}$ into $\mathsf{Span}(\mathbf{B} \mid \mathbf{B}_0 \mid \mathbf{B}_1)$. The span of $\mathbf{B}^{\perp}$ is decomposed into that of $\mathbf{B}_0^* \in \mathbb{Z}_q^{3k \times k}$ and $\mathbf{B}_1^* \in \mathbb{Z}_q^{3k \times k}$. An overview of the orthogonal relations between all these matrices is given in Figure 1.

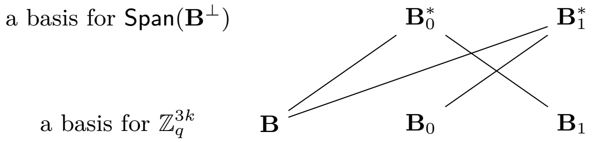
a basis for $\mathsf{Span}(\mathbf{B}^{\perp})$
$\mathbf{B}_0^*$
$\mathbf{B}_1^*$
a basis for $\mathbb{Z}_q^{3k}$
$\mathbf{B}$
$\mathbf{B}_0$
$\mathbf{B}_1$

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

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

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

### 1.3 More on Related Works

As we discussed before, there are different techniques [3,23,17,18,22] to achieve tight multi-challenge security for IBE schemes. Schemes in [18,22] are based on

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

the BKP framework and close to ours, while the other schemes are either using composite-order pairings [23] or based on stronger, non-standard assumptions [3,17]. We suppose the proof strategy in the work of Hofheinz, Jia, and Pan (HJP) [22] cannot be easily extended to randomize MAC tags for hierarchical identities, since their technique develops the random function $\mathsf{RF}_i$ in the full space $\mathbb{Z}_q$ and directly introduce randomness into $x'_0$. Inherently, in the HIBE setting, this strategy has the same limitation as BKP, namely, the outputs of $\mathsf{RF}_i$ and $\mathsf{RF}_{i+1}$ are both leaked when identities have different lengths. The work of Gong et al. [18] has the same issue as well. This limitation explains why some proof steps of LP HIBE schemes cannot be done in the multi-challenge setting, even with the HJP technique.

### 1.4 Open Problems

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

Another interesting direction is to make our schemes more efficient. A main disadvantage of our schemes is that they require relatively large master public keys. More precisely, ignoring the small constant $k$, $\mathsf{mpk}$ contains either $\mathbf{O}(\alpha L^2)$ or $\mathbf{O}(\gamma L)$ group elements, because of the use of the LP technique [28]. An interesting open problem is to construct a tightly secure HIBE with shorter master public keys, probably first in the single-challenge setting. A similar interesting open problem is to shorten the size of either user secret keys or ciphertexts to have a more efficient, tightly secure HIBE scheme in the multi-challenge setting.

### 1.5 Roadmap

We recall useful definitions in Section 2. Section 3 proposes affine MACs that can be used to construct tightly multi-challenge secure IBE and HIBE, respectively. It presents our core techniques as described above in a detailed and formal manner. Section 4 gives a transformation to HIBE, similar to the BKP framework. Its security proof is in the full version. For completeness of our claims, in the full version, we constructs an anonymous HIBE and a CCA-secure HIBE tightly in the multi-challenge setting. Furthermore, concrete instantiations of our schemes can be found in the full version as well.

## 2 Preliminaries

Notations. We use $x \xleftarrow{\$} \mathcal{S}$ to denote the process of sampling an element $x$ from $\mathcal{S}$ uniformly at random if $\mathcal{S}$ is a set and to denote the process of running $\mathcal{S}$ with its internal randomness and assign the output to $x$ if $\mathcal{S}$ is an algorithm. The expression $a \overset{?}{=} b$ stands for comparing $a$ and $b$ on equality and returning the result in Boolean value. For positive integers $k, \eta \in \mathbb{N}_+$ and a matrix $\mathbf{A} \in \mathbb{Z}_q^{(k+\eta)\times k}$, we denote the upper square matrix of $\mathbf{A}$ by $\overline{\mathbf{A}} \in \mathbb{Z}_q^{k \times k}$ and the lower $\eta$ 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 $\eta$ elements of $\mathbf{v}$ by $\underline{\mathbf{v}} \in \mathbb{Z}_q^\eta$. We use $\mathbf{A}^{-\top}$ as shorthand for $\left(\mathbf{A}^{-1}\right)^\top$. For a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, we use $\mathsf{Span}(\mathbf{A}) := \left\{\mathbf{Av} \mid \mathbf{v} \in \mathbb{Z}_q^m\right\}$ to denote the linear span of $\mathbf{A}$ and $\mathbf{A}^\perp$ denotes an arbitrary matrix with $\mathsf{Span}\left(\mathbf{A}^\perp\right) = \left\{\mathbf{v} \mid \mathbf{A}^\top \mathbf{v} = \mathbf{0}\right\}$.

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

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

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

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

### 2.1 Pairing Groups and Matrix Diffie-Hellman Assumptions

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

We use the implicit representation of group elements as in [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 ($\mathsf{MDDH}$) 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 *($\mathcal{D}_{\ell,k}$-$\mathsf{MDDH}$)* assumption *holds relative to* $\mathsf{PGGen}$ *in group $\mathbb{G}_s$ if for all PPT adversaries $\mathcal{A}$, it holds that*

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

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

The uniform distribution is a particular matrix distribution that deserves special attention, as an adversary breaking the $\mathcal{U}_{\ell,k}$ assumption can also distinguish between real $\mathsf{MDDH}$ tuples and random tuples for all other possible matrix distributions. For uniform distributions, they stated in [11] that $\mathcal{U}_k$-$\mathsf{MDDH}$ and $\mathcal{U}_{\ell,k}$-$\mathsf{MDDH}$ 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 ($\mathcal{U}_{\ell,k}$-$\mathsf{MDDH}$ $\Leftrightarrow$ $\mathcal{U}_k$-$\mathsf{MDDH}$ [11]).** *Let $\ell, k \in \mathbb{N}_+$ with $\ell > k$. An $\mathcal{U}_{\ell,k}$-$\mathsf{MDDH}$ instance is as hard as an $\mathcal{U}_k$-$\mathsf{MDDH}$ instance. More precisely, for each adversary $\mathcal{A}$ there exists an adversary $\mathcal{B}$ and vice versa with*

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

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

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

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

**Lemma 2 ($\mathcal{D}_{\ell,k}$-$\mathsf{MDDH} \Rightarrow \mathcal{U}_k$-$\mathsf{MDDH}$ [10]).** *Let $\ell, k \in \mathbb{N}_+$ with $\ell > k$ and let $\mathcal{D}_{\ell,k}$ be a matrix distribution. A $\mathcal{U}_k$-$\mathsf{MDDH}$ instance is at least as hard as an $\mathcal{D}_{\ell,k}$ instance. More precisely, for each adversary $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

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

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

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

**Lemma 3 (Random Self-reducibility [10]).** *For $\ell > k$ and any matrix distribution $\mathcal{D}_{\ell,k}$, the $\mathcal{D}_{\ell,k}$-$\mathsf{MDDH}$ assumption is random self-reducible. In particular, for any $Q \in \mathbb{N}_+$ and any adversary $\mathcal{A}$ there exists an adversary $\mathcal{B}$ with*

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

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

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

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

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

**Lemma 4.**

$$\Pr\left[\operatorname{rank}(\mathbf{A}) = k \mid \mathbf{A} \overset{\$}{\leftarrow} \mathbb{Z}_q^{k\times k}\right] \ge 1 - \frac{1}{q-1}$$

A proof can be found in the full version.

## 2.2 Pseudorandom Functions

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

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

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

The security notion for pseudorandom functions is pseudorandomness.

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

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

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

### 2.3 Affine MACs

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

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

**Definition 6 (Affine MAC with Levels).** *An* affine MAC with levels $\mathsf{MAC}$ *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* $\mathsf{sk}_{\mathsf{MAC}} := \Big(\mathbf{B}, (\mathbf{X}_{l,i,j})_{1 \le l \le \ell(p), 1 \le i \le L, 1 \le j \le \ell'(l,i)}, \mathbf{x}'\Big)$ *where* $\mathbf{B} \in \mathbb{Z}_q^{n \times n'}$, $\mathbf{X}_{l,i,j} \in \mathbb{Z}_q^{\eta \times n}$ *for* $l \in \{1, \dots, \ell(L)\}$, $i \in \{1, \dots, L\}$*, and* $j \in \{0, \dots, \ell'(l,i)\}$ *and* $\mathbf{x}' \in \mathbb{Z}_q^{\eta}$.
- $\mathsf{Tag}\big(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m} \in \mathcal{S}^{p \le L}\big)$ *returns a tag* $\tau := \Big(([\mathbf{t}_l]_2)_{1 \le l \le \ell(p)}, [\mathbf{u}]_2\Big)$ *where*

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

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

```
$\underline{\textsc{Init}_{\mathsf{MAC}}:}$
$\mathcal{PG} \overset{\$}{\leftarrow} \mathsf{PGGen}\left(1^{\lambda}\right)$
$\textbf{parse } \mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
$\mathsf{sk}_{\mathsf{MAC}} \overset{\$}{\leftarrow} \mathsf{Gen}_{\mathsf{MAC}}(\mathbb{G}_2, q, P_2)$
$\textbf{parse } \mathsf{sk}_{\mathsf{MAC}} =: \left(\mathbf{B}, (\mathbf{X}_j)_{1 \le j \le \ell}, \mathbf{x}'\right)$
$\textbf{return } \mathcal{PG}$

$\underline{\textsc{Eval}(\mathsf{m} \in \mathcal{S}):}$
$\mathcal{Q}_{\mathcal{M}} := \mathcal{Q}_{\mathcal{M}} \cup \{\mathsf{m}\}$
$\textbf{return } \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m})$

$\underline{\textsc{Finalize}_{\mathsf{MAC}}(\beta \in \{0,1\}):}$
$\textbf{return } (\mathcal{C}_{\mathcal{M}} \cap \mathcal{Q}_{\mathcal{M}} = \emptyset) \wedge \beta$
```

```
$\underline{\textsc{Chal}(\mathsf{m}^{\star} \in \mathcal{S}):}$
$\mathcal{C}_{\mathcal{M}} := \mathcal{C}_{\mathcal{M}} \cup \{\mathsf{m}^{\star}\}$
$\mathbf{h} \overset{\$}{\leftarrow} \mathbb{Z}_q^{\eta}$
$\mathbf{h}_0 := \left(\sum_{j=1}^{\ell} f_j(\mathsf{m}^{\star}) \mathbf{X}_j^{\top}\right) \mathbf{h}$
$\boxed{\mathbf{h}_0 \overset{\$}{\leftarrow} \mathbb{Z}_q^{n}}$
$h_1 = (\mathbf{x}')^{\top} \mathbf{h} \in \mathbb{Z}_q$
$\boxed{h_1 \overset{\$}{\leftarrow} \mathbb{Z}_q}$
$\textbf{return } \left([\mathbf{h}]_1, [\mathbf{h}_0]_1, [h_1]_T\right)$
```

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

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

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

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

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

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

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

*is negligible.*

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

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

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

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

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

# 3 Delegatable Affine MACs with Tight Multi-Challenge Security.

## 3.1 Warm-up: IBE

First, we present the technique to handle multiple challenge queries in the IBE setting ($L = 1$). The MAC is given in Figure 4. This affine MAC has identity space $\mathcal{S} = \{0,1\}^{\alpha}$ (for arbitrary $\alpha \in \mathbb{N}_+$) and uses $n = 2k$, $n' = k$, $\eta = k$ and $\ell' = \alpha$. To match the formal definition, $\mathbf{X}_{j,b}$ should be renamed to $\mathbf{X}_{2j-b}$ and $f_{2j-b}(\mathsf{m}) := \Big(\mathsf{m}_j \overset{?}{=} b\Big)$. The MAC looks very similar to the one in [22] and achieves the same security and very similar efficiency, however the security proof is quite different. A comparison of the resulting IBE with other tightly secure IBEs can be found in Table 2.

As in [22], we need to ensure that the adversary can only query one tag per message. The key generator can ensure this by making the tags deterministic. He can achieve this by storing the generated tags for duplicated queries (stateful scheme) or by generating the randomness with a pseudorandom function. We have done the later in our presentation. The affine MACs with levels we present later solve this by having rerandomizable tags. Of course, they can be used as affine MAC as well by setting $L = 1$, but this comes at the cost of being slightly less efficient.

| Scheme | A | $\|\mathsf{mpk}\|$ | $\|\mathsf{usk}\|$ | $\|\mathsf{C}\|$ | Loss | MC | Ass. |
|---|---|---|---|---|---|---|---|
| CW13 [8] | ✗ | $2k^2(2n+1)\|\mathbb{G}_1\|+k\|\mathbb{G}_T\|$ | $4k\|\mathbb{G}_2$ | $4k\|\mathbb{G}_1$ | $\mathbf{O}(n)$ | ✗ | $k$-LIN |
| BKP14 [5] | ✓ | $(2nk^2+2k)\mathbb{G}_1\|$ | $(2k+1)\|\mathbb{G}_2\|$ | $(2k+1)\|\mathbb{G}_1\|$ | $\mathbf{O}(\lambda)$ | ✗ | $k$-LIN |
| AHY15 [3] | ✓ | $(16n+8)\|\mathbb{G}_1\|+2\|\mathbb{G}_T\|$ | $8\|\mathbb{G}_2\|$ | $8\|\mathbb{G}_1\|$ | $\mathbf{O}(n)$ | ✓ | DLIN |
| GCD$^+$16$_1$ [17] | ✗ | $(6nk^2+3k^2)\|\mathbb{G}_1\|+k\|\mathbb{G}_T\|$ | $6k\|\mathbb{G}_2\|$ | $6k\|\mathbb{G}_1\|$ | $\mathbf{O}(n)$ | ✓ | $k$-LIN |
| GCD$^+$16$_2$ [17] | ✗ | $(4nk^2+2k^2)\|\mathbb{G}_1\|+k\|\mathbb{G}_T\|$ | $4k\|\mathbb{G}_2\|$ | $4k\|\mathbb{G}_1\|$ | $\mathbf{O}(n)$ | ✓ | $k$-LINAI |
| GDCC16 [18] | ✓ | $(2nk^2+3k^2)\|\mathbb{G}_1\|+k\|\mathbb{G}_T\|$ | $4k\|\mathbb{G}_2\|$ | $4k\|\mathbb{G}_1\|$ | $\mathbf{O}(n)$ | ✓ | $k$-LIN |
| HJP18 [22] | ✓ | $((3+n)k^2+k)\|\mathbb{G}_1\|$ | $4k\|\mathbb{G}_2\|$ | $4k\|\mathbb{G}_1\|$ | $\mathbf{O}(n)$ | ✓ | $k$-LIN |
| Ours | ✓ | $((2+2n)k^2+k)\|\mathbb{G}_1\|$ | $4k\|\mathbb{G}_2\|$ | $4k\|\mathbb{G}_1\|$ | $\mathbf{O}(n)$ | ✓ | $k$-LIN |

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

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

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

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

**Fig. 4.** The new multi-challenge tightly secure affine MAC $\mathsf{MAC}_{mc}$.

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

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

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

*Proof.* The proof uses a hybrid argument with the hybrids $\mathsf{G}_0$, $\mathsf{G}_1$, $\mathsf{G}_{2,\hat{\jmath},0}$ for $\hat{\jmath} \in \{0, \dots, \alpha\}$, $\mathsf{G}_{2,\hat{\jmath},1}$–$\mathsf{G}_{2,\hat{\jmath},3}$ for $\hat{\jmath} \in \{0, \dots, \alpha - 1\}$ and finally $\mathsf{G}_3$–$\mathsf{G}_5$. They are given in Table 3. They make use of the random functions $\mathsf{RF} : \mathcal{S} \to \mathbb{Z}_q^{2k}$, $\mathsf{RF}' : \mathcal{S} \to \mathbb{Z}_q^k$, $\mathsf{RF}_{\hat{\jmath}} : \{0,1\}^{\hat{\jmath}} \to \mathbb{Z}_q^{k \times 2k}$, $\mathsf{ZF}_{\hat{\jmath}} : \{0,1\}^{\hat{\jmath}} \to \mathbb{Z}_q^{k \times k}$ and $\mathsf{OF}_{\hat{\jmath}} : \{0,1\}^{\hat{\jmath}} \to \mathbb{Z}_q^{k \times k}$ for $\hat{\jmath} \in \{1, \dots, \alpha\}$ and $\widetilde{\mathsf{RF}} : \mathcal{S} \to \mathbb{Z}_q^k$.

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

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

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

*Proof.* The value $\mathbf{t}$ for in the Eval oracle is chosen randomly in game $\mathsf{G}_1$ instead of pseudorandom in game $\mathsf{G}_0$. This leads to a straight forward reduction to the pseudorandomness of $\mathcal{F} := (\mathsf{Gen}_{\mathsf{PRF}}, \mathsf{PRF})$. □

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

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

*Proof.* In game $\mathsf{G}_1$ replace $\mathbf{X}_{1,b}$ with $\mathbf{X}_{1,b} + \mathsf{RF}_0(\varepsilon)$ for $b \in \{0,1\}$ to obtain game $\mathsf{G}_{2,0,0}$. □

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

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

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

A proof can be found in the full version.

```
$\mathsf{G}_0$ | $\mathsf{G}_1$  $\mathsf{G}_{2,\hat{\jmath},0}$  $\boxed{\mathsf{G}_{2,\hat{\jmath},1}\ \boxed{\mathsf{G}_{2,\hat{\jmath},2}}\ \boxed{\mathsf{G}_{2,\hat{\jmath},3}}}$  $\boxed{\mathsf{G}_3\ \boxed{\mathsf{G}_4\ \boxed{\mathsf{G}_5}}}$

Init_MAC:
    $\mathcal{PG} \xleftarrow{\$} \mathsf{PGGen}(1^\lambda)$
    parse $\mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
    $\boxed{\mathbf{B}_0, \mathbf{B}_1 \xleftarrow{\$} \mathcal{U}_{2k,k} \text{ such that } \mathbf{B}_0, \mathbf{B}_1 \text{ is a basis of } \mathbb{Z}_q^{2k}}$
    $\mathcal{K} \xleftarrow{\$} \mathsf{Gen}_{\mathsf{PRF}}(1^\lambda)$
    for $j \in \{1, \ldots, \alpha\},\ b \in \{0,1\}$ do
        $\mathbf{X}_{j,b} \xleftarrow{\$} \mathbb{Z}_q^{k \times 2k}$
    $\mathbf{x}' \xleftarrow{\$} \mathbb{Z}_q^k$
    return $\mathcal{PG}$

Chal($\mathsf{m}^\star \in \mathcal{S}$):
    $\mathcal{C}_{\mathcal{M}} := \mathcal{C}_{\mathcal{M}} \cup \{\mathsf{m}^\star\}$
    $\mathbf{h} \xleftarrow{\$} \mathbb{Z}_q^k$
    $\mathbf{h}_0 := \sum_{j=1}^{\alpha} \mathbf{X}_{j,\mathsf{m}^\star_j}^\top \mathbf{h}$
        $+ \mathsf{RF}_{\hat{\jmath}}(\mathsf{m}^\star_{|\hat{\jmath}})^\top \mathbf{h}$
        $\boxed{+ \left(\mathbf{B}_1^\perp \mathsf{ZF}_{\hat{\jmath}+1}(\mathsf{m}^\star_{|\hat{\jmath}+1})^\top + \mathbf{B}_0^\perp \mathsf{OF}_{\hat{\jmath}}(\mathsf{m}^\star_{|\hat{\jmath}})^\top\right)\mathbf{h}}$
        $\boxed{+ \left(\mathbf{B}_1^\perp \mathsf{ZF}_{\hat{\jmath}+1}(\mathsf{m}^\star_{|\hat{\jmath}+1})^\top + \mathbf{B}_0^\perp \mathsf{OF}_{\hat{\jmath}+1}(\mathsf{m}^\star_{|\hat{\jmath}+1})^\top\right)\mathbf{h}}$
        $\boxed{+ \mathsf{RF}_\alpha(\mathsf{m}^\star)^\top \mathbf{h}}$
    $\boxed{\mathbf{h}_0 \xleftarrow{\$} \mathbb{Z}_q^{2k}}$
    $h_1 := (\mathbf{x}')^\top \mathbf{h}$
    $\boxed{h_1 \xleftarrow{\$} \mathbb{Z}_q}$
    return $([\mathbf{h}]_1, [\mathbf{h}_0]_1, [h_1]_T)$

Eval($\mathsf{m} \in \mathcal{S}$):
    $\mathcal{Q}_{\mathcal{M}} := \mathcal{Q}_{\mathcal{M}} \cup \{\mathsf{m}\}$
    $\mathbf{t} := \mathsf{PRF}_{\mathcal{K}}(\mathsf{m}) \in \mathbb{Z}_q^{2k}$
    $\boxed{\mathbf{t} := \mathsf{RF}(\mathsf{m}) \in \mathbb{Z}_q^{2k}}$
    $\boxed{\mathbf{s} := \mathsf{RF}'(\mathsf{m}) \in \mathbb{Z}_q^k}$
    if $\mathsf{m}_{\hat{\jmath}+1} = 0$ then
        $\mathbf{t} := \mathbf{B}_0\mathbf{s}$
    else
        $\mathbf{t} := \mathbf{B}_1\mathbf{s}$
    $\mathbf{u} := \sum_{j=1}^{\alpha} \mathbf{X}_{j,\mathsf{m}_j}\mathbf{t} + \mathbf{x}'$
        $+ \mathsf{RF}_{\hat{\jmath}}(\mathsf{m}_{|\hat{\jmath}})\mathbf{t}$
        $\boxed{+ \left(\mathsf{ZF}_{\hat{\jmath}+1}(\mathsf{m}_{|\hat{\jmath}+1})(\mathbf{B}_1^\perp)^\top + \mathsf{OF}_{\hat{\jmath}}(\mathsf{m}_{|\hat{\jmath}})(\mathbf{B}_0^\perp)^\top\right)\mathbf{t}}$
        $\boxed{+ \left(\mathsf{ZF}_{\hat{\jmath}+1}(\mathsf{m}_{|\hat{\jmath}+1})(\mathbf{B}_1^\perp)^\top + \mathsf{OF}_{\hat{\jmath}+1}(\mathsf{m}_{|\hat{\jmath}+1})(\mathbf{B}_0^\perp)^\top\right)\mathbf{t}}$
    $\boxed{\mathbf{u} := \widetilde{\mathsf{RF}}(\mathsf{m})}$
    return $([\mathbf{t}]_2, [\mathbf{u}]_2)$

Finalize_MAC($\beta \in \{0,1\}$):
    return $(\mathcal{C}_{\mathcal{M}} \cap \mathcal{Q}_{\mathcal{M}} = \emptyset) \wedge \beta$
```

**Fig. 5.** Hybrids for the security proof of $\mathsf{MAC}_{mc}$.

| Hybrid | $\mathbf{t}$ uniform in | $r_{\mathbf{u}}(\mathsf{m})$ | $r_{\mathbf{h}_0}(\mathsf{m})$ | Transition |
|---|---|---|---|---|
| $\mathsf{G}_0$ | $\mathbb{Z}_q^{2k}$ (pseudorandom) | $0$ | | Original game |
| $\mathsf{G}_1$ | $\mathbb{Z}_q^{2k}$ | $0$ | | $\mathsf{PRF}$ |
| $\mathsf{G}_{2,\hat{\jmath},0}$ | $\mathbb{Z}_q^{2k}$ | $\mathsf{RF}_{\hat{\jmath}}\big(\mathsf{m}_{\vert\hat{\jmath}}\big)$ | | Identical |
| $\mathsf{G}_{2,\hat{\jmath},1}$ | **if** $\mathsf{m}_{\hat{\jmath}+1} = 0$ **then**<br>$\vert\,\mathsf{Span}(\mathbf{B}_0)$<br>**else**<br>$\lfloor \mathsf{Span}(\mathbf{B}_1)$ | $\mathsf{RF}_{\hat{\jmath}}\big(\mathsf{m}_{\vert\hat{\jmath}}\big)$ | | $\mathcal{U}_k$-$\mathsf{MDDH}$ in $\mathbb{G}_2$ |
| $\mathsf{G}_{2,\hat{\jmath},2}$ | | $\Big(\mathsf{ZF}_{\hat{\jmath}+1}\big(\mathsf{m}_{\vert\hat{\jmath}+1}\big)\big(\mathbf{B}_1^{\perp}\big)^{\top} + \mathsf{OF}_{\hat{\jmath}}\big(\mathsf{m}_{\vert\hat{\jmath}}\big)\big(\mathbf{B}_0^{\perp}\big)^{\top}\Big)$ | | $\mathcal{U}_k$-$\mathsf{MDDH}$ in $\mathbb{G}_1$ |
| $\mathsf{G}_{2,\hat{\jmath},3}$ | | $\Big(\mathsf{ZF}_{\hat{\jmath}+1}\big(\mathsf{m}_{\vert\hat{\jmath}+1}\big)\big(\mathbf{B}_1^{\perp}\big)^{\top} + \mathsf{OF}_{\hat{\jmath}+1}\big(\mathsf{m}_{\vert\hat{\jmath}+1}\big)\big(\mathbf{B}_0^{\perp}\big)^{\top}\Big)$ | | $\mathcal{U}_k$-$\mathsf{MDDH}$ in $\mathbb{G}_1$ |
| $\mathsf{G}_{2,\hat{\jmath}+1,0}$ | $\mathbb{Z}_q^{2k}$ | $\mathsf{RF}_{\hat{\jmath}+1}\big(\mathsf{m}_{\vert\hat{\jmath}+1}\big)$ | | $\mathcal{U}_k$-$\mathsf{MDDH}$ in $\mathbb{G}_2$ |
| $\mathsf{G}_3$ | $\mathbb{Z}_q^{2k}$ | uniform random | $\mathsf{RF}_{\alpha}(\mathsf{m})$ | Statistically close |
| $\mathsf{G}_4$ | $\mathbb{Z}_q^{2k}$ | uniform random | uniform random | $\mathcal{U}_k$-$\mathsf{MDDH}$ in $\mathbb{G}_1$ |
| $\mathsf{G}_5$ | $\mathbb{Z}_q^{2k}$ | uniform random | uniform random | $\mathcal{U}_k$-$\mathsf{MDDH}$ in $\mathbb{G}_1$ |

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

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

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

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

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

Define

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

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

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

```
$\underline{\textsc{Init}_{\mathsf{MAC}}:}$
parse $\mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
$\mathbf{B}_0, \mathbf{B}_1 \xleftarrow{\$} \mathcal{U}_{2k,k}$
such that $\mathbf{B}_0, \mathbf{B}_1$ is a basis of $\mathbb{Z}_q^{2k}$
for $j \in \{1, \ldots, \alpha\},\ b \in \{0,1\}$ do
    $\mathbf{J}_{j,b} \xleftarrow{\$} \mathbb{Z}_q^{k \times 2k}$
    if $(j,b) \neq (\hat{\jmath}+1, 1)$ then $\mathbf{X}_{j,b} := \mathbf{J}_{j,b}$
// Implicit: $\mathbf{X}_{\hat{\jmath}+1,1} := \mathbf{J}_{\hat{\jmath}+1,1} + \left(\mathbf{B}_1^{\perp}\underline{\mathbf{D}}\overline{\mathbf{D}}^{-1}\right)^{\top}$
$\mathbf{x}' \xleftarrow{\$} \mathbb{Z}_q^k$
return $\mathcal{PG}$

$\underline{\textsc{Eval}(\mathsf{m} \in \mathcal{S}):}$
$\mathcal{Q}_{\mathcal{M}} := \mathcal{Q}_{\mathcal{M}} \cup \{\mathsf{m}\}$
$\mathbf{s} := \mathsf{RF}'(\mathsf{m}) \in \mathbb{Z}_q^k$
if $\mathsf{m}_{\hat{\jmath}+1} = 0$ then
    $\mathbf{t} := \mathbf{B}_0\mathbf{s}$
else
    $\mathbf{t} := \mathbf{B}_1\mathbf{s}$
$\mathbf{u} := \Bigg(\sum_{j=1}^{\alpha} \mathbf{J}_{j,\mathsf{m}_j} + \mathsf{ZF}_{\hat{\jmath}}\left(\mathsf{m}_{|\hat{\jmath}}\right)\left(\mathbf{B}_1^{\perp}\right)^{\top}$
        $+ \mathsf{OF}_{\hat{\jmath}}\left(\mathsf{m}_{|\hat{\jmath}}\right)\left(\mathbf{B}_0^{\perp}\right)^{\top}\Bigg)\mathbf{t} + \mathbf{x}'$
return $\left([\mathbf{t}]_2, [\mathbf{u}]_2\right)$
```

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

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

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

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

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

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

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

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

with

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

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

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

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

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

*Proof.* We define

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

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

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

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

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

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

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

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

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

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

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

The remaining transition is the reverse of Lemma 7. □

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

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

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

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

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

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

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

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

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

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

```
$\underline{\textsc{Init}_{\mathsf{MAC}}:}$
$\textbf{parse } \mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
$\mathbf{B}_0, \mathbf{B}_1 \overset{\$}{\leftarrow} \mathcal{U}_{2k,k}$
such that $\mathbf{B}_0, \mathbf{B}_1$ is a basis of $\mathbb{Z}_q^{2k}$
$\textbf{for } j \in \{1, \ldots, \alpha\},\ b \in \{0,1\} \textbf{ do}$
    $\mathbf{J}_{j,b} \overset{\$}{\leftarrow} \mathbb{Z}_q^{k \times 2k}$
    $\textbf{if } j \neq 1 \textbf{ then } \mathbf{X}_{j,b} := \mathbf{J}_{j,b}$
// Implicit: For $b \in \{0,1\}$ :
// $\mathbf{X}_{1,b} := \mathbf{J}_{1,b} + \left(\underline{\mathbf{D}}\overline{\mathbf{D}}^{-1}\right)^\top$
$\mathbf{x}' \overset{\$}{\leftarrow} \mathbb{Z}_q^k$
$\textbf{return } \mathcal{PG}$

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

$\underline{\textsc{Eval}(\mathsf{m} \in \mathcal{S}):}$
$\mathcal{Q}_\mathcal{M} := \mathcal{Q}_\mathcal{M} \cup \{\mathsf{m}\}$
$\mathbf{t} := \mathsf{RF}(\mathsf{m}) \in \mathbb{Z}_q^{2k}$
$\mathbf{u} := \widetilde{\mathsf{RF}}(\mathsf{m})$
$\textbf{return } \left([\mathbf{t}]_2, [\mathbf{u}]_2\right)$

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

**Fig. 7.** Reduction for the transition from $\mathsf{G}_3$ to $\mathsf{G}_4$ to the $Q_c$-fold $\mathcal{U}_{3k,k}$-$\mathsf{MDDH}$ challenge $\left([\mathbf{D}]_1, [\mathbf{f}_1]_1, \ldots, [\mathbf{f}_{Q_c}]_1\right)$.

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

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

If $\mathbf{r}_c = \mathbf{0}$, we are simulating game $\mathsf{G}_3$. If $\mathbf{r}_c$ is uniform random, then $\mathbf{h}_0$ is uniform random and we are simulating game $\mathsf{G}_4$. □

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

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

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

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

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

```
$\underline{\textsc{Init}_{\mathsf{MAC}}:}$
$\mathbf{parse}\ \mathcal{PG} =: (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$
$\mathbf{B}_0, \mathbf{B}_1 \xleftarrow{\$} \mathcal{U}_{2k,k}$
such that $\mathbf{B}_0, \mathbf{B}_1$ is a basis of $\mathbb{Z}_q^{2k}$
$\mathbf{for}\ j \in \{1, \ldots, \alpha\},\ b \in \{0,1\}\ \mathbf{do}$
    $\mathbf{X}_{j,b} \xleftarrow{\$} \mathbb{Z}_q^{k \times 2k}$
$\mathbf{j}' \xleftarrow{\$} \mathbb{Z}_q^k$
// Implicit: $\mathbf{x}' := \mathbf{j}' + \left(\underline{\mathbf{D}}\overline{\mathbf{D}}^{-1}\right)^\top$
$\mathbf{return}\ \mathcal{PG}$

$\underline{\textsc{Finalize}_{\mathsf{MAC}}(\beta \in \{0,1\}):}$
$\mathbf{return}\ (\mathcal{C}_{\mathcal{M}} \cap \mathcal{Q}_{\mathcal{M}} = \emptyset) \land \beta$
```

```
$\underline{\textsc{Eval}(\mathsf{m} \in \mathcal{S}):}$
$\mathcal{Q}_{\mathcal{M}} := \mathcal{Q}_{\mathcal{M}} \cup \{\mathsf{m}\}$
$\mathbf{t} := \mathsf{RF}(\mathsf{m}) \in \mathbb{Z}_q^{2k}$
$\mathbf{u} := \widetilde{\mathsf{RF}}(\mathsf{m})$
$\mathbf{return}\ \left([\mathbf{t}]_2, [\mathbf{u}]_2\right)$

$\underline{\textsc{Chal}(\mathsf{m}^\star \in \mathcal{S}):}$
$\mathcal{C}_{\mathcal{M}} := \mathcal{C}_{\mathcal{M}} \cup \{\mathsf{m}^\star\}$
Let this be the $c$-th Chal query.
$\mathbf{h} := \overline{\mathbf{f}_c}$
$\mathbf{h}_0 \xleftarrow{\$} \mathbb{Z}_q^{2k}$
$h_1 := (\mathbf{j}')^\top \mathbf{h} + \underline{\mathbf{f}_c}$
$\mathbf{return}\ \left([\mathbf{h}]_1, [\mathbf{h}_0]_1, [h_1]_T\right)$
```

**Fig. 8.** Reduction for the transition from $\mathsf{G}_4$ to $\mathsf{G}_5$ to the $Q_c$-fold $\mathcal{U}_k$-MDDH challenge $\left([\mathbf{D}]_1, [\mathbf{f}_1]_1, \ldots, [\mathbf{f}_{Q_c}]_1\right)$.

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

The value $h_1$ is calculated as

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

If $r_c = 0$, we are simulating game $\mathsf{G}_4$. If $r_c$ is uniform random, then $h_1$ is uniform random and we are simulating game $\mathsf{G}_5$. □

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

### 3.2 Tight Multi-challenge Security for the first LP MAC

Here we show how tight multi-challenge security can be obtained for the first HIBE from [28]. The MAC, given in Figure 9, only differs in the parameter $\eta$, that is $k$ here. Furthermore this MAC has identity space base set $\mathcal{S} = \{0,1\}^\alpha$ (for arbitrary $\alpha \in \mathbb{N}_+$) and uses $n = 3k$, $n' = k$, $\ell(p) = 1$ (thus also satisfies the delegatable, affine MAC notion) and $\ell'(l,i) = 2i\alpha$. To match the formal definition, $\mathbf{X}_{i,j,b}$ should be renamed to $\mathbf{X}_{i,2j-b}$ and $f_{i,2j-b}(\mathsf{m}) := \left(\llbracket \mathsf{m}_{|i} \rrbracket_j \overset{?}{=} b\right)$. In the single-challenge setting, all of these transitions are information-theoretic secure, but in the multi-challenge setting we need a $\mathsf{MDDH}$-assumption in $\mathbb{G}_1$ to proof them.

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

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

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

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

**Fig. 9.** The new multi-challenge tightly secure delegatable affine MAC $\mathsf{MAC}_1$.

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

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

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

The proof can be found in the full version. A summary of the hybrids can be found in Table 4.

### 3.3 Tight Multi-challenge Security for the second LP MAC

The second MAC of [28] can be made tightly secure in a similar way to the first MAC. Details can be found in the full version.

## 4 Transformation to HIBE

Any mHPR-CMA affine MAC with levels can be tightly transformed to an hierarchical identity-based key encapsulation mechanism (HIBKEM) under the

| Hybrid | $\mathbf{t}$ uniform in | $r_{\mathbf{u}}(\mathsf{m})$ | $r_{\mathbf{h}_0}(\mathsf{m})$ | Transition |
|---|---|---|---|---|
| $\mathsf{G}_0$ | $\mathsf{Span}(\mathbf{B})$ | $0$ | | Original game |
| $\mathsf{G}_1$ | $\mathsf{Span}(\mathbf{B})$ | $0$ | | Identical |
| $\mathsf{G}_{2,\hat{\imath},0}$ | $\mathsf{Span}(\mathbf{B})$ | $0$ | | Identical |
| $\mathsf{G}_{2,\hat{\imath},1}$ | $\mathbb{Z}_q^{3k}$ | $0$ | | $\mathcal{U}_k$-$\mathsf{MDDH}$ in $\mathbb{G}_2$ |
| $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},0}$ | $\mathbb{Z}_q^{3k}$ | $\mathsf{RF}_{\hat{\imath},\hat{\jmath}}\left([\![\mathsf{m}]\!]_{\|\hat{\jmath}}\right)\left(\mathbf{B}^{\perp}\right)^{\top}$ | | Identical |
| $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},1}$ | **if** $[\![\mathsf{m}]\!]_{\hat{\jmath}+1} = 0$ **then**<br>$\mid \mathsf{Span}(\mathbf{B}\|\mathbf{B}_0)$<br>**else**<br>$\lfloor \mathsf{Span}(\mathbf{B}\|\mathbf{B}_1)$ | $\mathsf{RF}_{\hat{\imath},\hat{\jmath}}\left([\![\mathsf{m}]\!]_{\|\hat{\jmath}}\right)\left(\mathbf{B}^{\perp}\right)^{\top}$ | | $\mathcal{U}_k$-$\mathsf{MDDH}$ in $\mathbb{G}_2$ |
| $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},2}$ | | $\Big(\mathsf{ZF}_{\hat{\imath},\hat{\jmath}+1}\left([\![\mathsf{m}]\!]_{\|\hat{\jmath}+1}\right)(\mathbf{B}_0^*)^{\top}$<br>$+\,\mathsf{OF}_{\hat{\imath},\hat{\jmath}}\left([\![\mathsf{m}]\!]_{\|\hat{\jmath}}\right)(\mathbf{B}_1^*)^{\top}\Big)$ | | $\mathcal{U}_k$-$\mathsf{MDDH}$ in $\mathbb{G}_1$ |
| $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath},3}$ | | $\Big(\mathsf{ZF}_{\hat{\imath},\hat{\jmath}+1}\left([\![\mathsf{m}]\!]_{\|\hat{\jmath}+1}\right)(\mathbf{B}_0^*)^{\top}$<br>$+\,\mathsf{OF}_{\hat{\imath},\hat{\jmath}+1}\left([\![\mathsf{m}]\!]_{\|\hat{\jmath}+1}\right)(\mathbf{B}_1^*)^{\top}\Big)$ | | $\mathcal{U}_k$-$\mathsf{MDDH}$ in $\mathbb{G}_1$ |
| $\mathsf{G}_{2,\hat{\imath},2,\hat{\jmath}+1,0}$ | $\mathbb{Z}_q^{3k}$ | $\mathsf{RF}_{\hat{\imath},\hat{\jmath}+1}\left([\![\mathsf{m}]\!]_{\|\hat{\jmath}+1}\right)\left(\mathbf{B}^{\perp}\right)^{\top}$ | | $\mathcal{U}_k$-$\mathsf{MDDH}$ in $\mathbb{G}_2$ |
| $\mathsf{G}_{2,\hat{\imath},3}$ | $\mathbb{Z}_q^{3k}$ | uniform random | $\mathsf{RF}_{\hat{\imath}}\left(\mathsf{m}_{\|\hat{\imath}}\right)\left(\mathbf{B}^{\perp}\right)^{\top}$ | Statistically close |
| $\mathsf{G}_{2,\hat{\imath},4}$ | $\mathbb{Z}_q^{3k}$ | uniform random | $0$ | $\mathcal{U}_k$-$\mathsf{MDDH}$ in $\mathbb{G}_1$ |
| $\mathsf{G}_{2,\hat{\imath},5}$ | $\mathsf{Span}(\mathbf{B})$ | uniform random | $0$ | $\mathcal{U}_k$-$\mathsf{MDDH}$ in $\mathbb{G}_2$ |
| $\mathsf{G}_3$ | $\mathsf{Span}(\mathbf{B})$ | uniform random | $0$ | $\mathcal{U}_k$-$\mathsf{MDDH}$ in $\mathbb{G}_1$ |

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

$\mathcal{D}_{k+\eta,k}$-$\mathsf{MDDH}$ assumption in $\mathbb{G}_1$ with the transformation given in Figure 10. The transformation follows the same idea as [5]. A security proof can be found in the full version. With a QANIZK for linear subspaces we can use the idea of [22] to obtain an $\mathsf{IND}$-$\mathsf{HID}$-$\mathsf{CCA}$-secure HIBE. Details can be found in the full version.

## References

1. Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Kohno, T., Lange, T., Malone-Lee, J., Neven, G., Paillier, P., Shi, H.: Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 205–222. Springer, Heidelberg (Aug 2005)
2. Abe, M., Jutla, C.S., Ohkubo, M., Pan, J., Roy, A., Wang, Y.: Shorter QA-NIZK and SPS with tighter security. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019, Part III. LNCS, vol. 11923, pp. 669–699. Springer, Heidelberg (Dec 2019)

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

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

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

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

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

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

3. Attrapadung, N., Hanaoka, G., Yamada, S.: A framework for identity-based encryption with almost tight security. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015, Part I. LNCS, vol. 9452, pp. 521–549. Springer, Heidelberg (Nov / Dec 2015)
4. Bellare, M., Goldwasser, S.: New paradigms for digital signatures and message authentication based on non-interative zero knowledge proofs. In: Brassard, G. (ed.) CRYPTO'89. LNCS, vol. 435, pp. 194–211. Springer, Heidelberg (Aug 1990)
5. Blazy, O., Kiltz, E., Pan, J.: (Hierarchical) identity-based encryption from affine message authentication. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014, Part I. LNCS, vol. 8616, pp. 408–425. Springer, Heidelberg (Aug 2014)
6. Blazy, O., Kiltz, E., Pan, J.: (Hierarchical) identity-based encryption from affine message authentication. Cryptology ePrint Archive, Report 2014/581 (2014), `http://eprint.iacr.org/2014/581`
7. Boneh, D., Franklin, M.K.: Identity-based encryption from the Weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (Aug 2001)
8. Chen, J., Wee, H.: Fully, (almost) tightly secure IBE and dual system groups. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part II. LNCS, vol. 8043, pp. 435–460. Springer, Heidelberg (Aug 2013)
9. Dodis, Y., Kiltz, E., Pietrzak, K., Wichs, D.: Message authentication, revisited. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 355–374. Springer, Heidelberg (Apr 2012)
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, Part II. LNCS, vol. 8043, pp. 129–147. Springer, Heidelberg (Aug 2013)
11. Gay, R., Hofheinz, D., Kiltz, E., Wee, H.: Tightly CCA-secure encryption without pairings. In: Fischlin, M., Coron, J.S. (eds.) EUROCRYPT 2016, Part I. LNCS, vol. 9665, pp. 1–27. Springer, Heidelberg (May 2016)
12. Gay, R., Hofheinz, D., Kohl, L.: Kurosawa-desmedt meets tight security. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017, Part III. LNCS, vol. 10403, pp. 133–160. Springer, Heidelberg (Aug 2017)
13. Gay, R., Hofheinz, D., Kohl, L., Pan, J.: More efficient (almost) tightly secure structure-preserving signatures. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018, Part II. LNCS, vol. 10821, pp. 230–258. Springer, Heidelberg (Apr / May 2018)
14. Gentry, C., Silverberg, A.: Hierarchical ID-based cryptography. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 548–566. Springer, Heidelberg (Dec 2002)
15. Gjøsteen, K., Jager, T.: Practical and tightly-secure digital signatures and authenticated key exchange. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018, Part II. LNCS, vol. 10992, pp. 95–125. Springer, Heidelberg (Aug 2018)
16. Gong, J., Cao, Z., Tang, S., Chen, J.: Extended dual system group and shorter unbounded hierarchical identity based encryption. Designs, Codes and Cryptography 80(3), 525–559 (Sep 2016), `https://doi.org/10.1007/s10623-015-0117-z`
17. Gong, J., Chen, J., Dong, X., Cao, Z., Tang, S.: Extended nested dual system groups, revisited. In: Cheng, C.M., Chung, K.M., Persiano, G., Yang, B.Y. (eds.) PKC 2016, Part I. LNCS, vol. 9614, pp. 133–163. Springer, Heidelberg (Mar 2016)
18. 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, Part II. LNCS, vol. 10032, pp. 624–654. Springer, Heidelberg (Dec 2016)

19. Groth, J., Sahai, A.: Efficient non-interactive proof systems for bilinear groups. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 415–432. Springer, Heidelberg (Apr 2008)
20. Hofheinz, D.: Adaptive partitioning. In: Coron, J., Nielsen, J.B. (eds.) EUROCRYPT 2017, Part III. LNCS, vol. 10212, pp. 489–518. Springer, Heidelberg (Apr / May 2017)
21. 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 (Aug 2012)
22. Hofheinz, D., Jia, D., Pan, J.: Identity-based encryption tightly secure under chosen-ciphertext attacks. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018, Part II. LNCS, vol. 11273, pp. 190–220. Springer, Heidelberg (Dec 2018)
23. 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 (Mar / Apr 2015)
24. Horwitz, J., Lynn, B.: Toward hierarchical identity-based encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 466–481. Springer, Heidelberg (Apr / May 2002)
25. Jutla, C.S., Roy, A.: Shorter quasi-adaptive NIZK proofs for linear subspaces. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part I. LNCS, vol. 8269, pp. 1–20. Springer, Heidelberg (Dec 2013)
26. Kiltz, E., Loss, J., Pan, J.: Tightly-secure signatures from five-move identification protocols. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017, Part III. LNCS, vol. 10626, pp. 68–94. Springer, Heidelberg (Dec 2017)
27. Kiltz, E., Wee, H.: Quasi-adaptive NIZK for linear subspaces revisited. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015, Part II. LNCS, vol. 9057, pp. 101–128. Springer, Heidelberg (Apr 2015)
28. Langrehr, R., Pan, J.: Tightly secure hierarchical identity-based encryption. In: Lin, D., Sako, K. (eds.) PKC 2019, Part I. LNCS, vol. 11442, pp. 436–465. Springer, Heidelberg (Apr 2019)
29. Langrehr, R., Pan, J.: Tightly secure hierarchical identity-based encryption. Cryptology ePrint Archive, Report 2019/058 (2019), https://eprint.iacr.org/2019/058
30. Lewko, A.B.: 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 (Apr 2012)
31. Lewko, A.B., Waters, B.: New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 455–479. Springer, Heidelberg (Feb 2010)
32. Lewko, A.B., 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 (May 2014)
33. 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)
34. 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 (Aug 2009)
35. Waters, B.R.: Efficient identity-based encryption without random oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (May 2005)