(Hierarchical) Identity-Based Encryption from Affine Message Authentication

Olivier Blazy Eike Kiltz Jiaxin Pan

Faculty of Mathematics
Horst Görtz Institute for IT-Security
Ruhr University Bochum, Germany
{olivier.blazy,eike.kiltz,jiaxin.pan}@rub.de

Abstract

We provide a generic transformation from any *affine* message authentication code (MAC) to an identity-based encryption (IBE) scheme over pairing groups of prime order. If the MAC satisfies a security notion related to unforgeability against chosen-message attacks and, for example, the k-Linear assumption holds, then the resulting IBE scheme is adaptively secure. Our security reduction is tightness preserving, i.e., if the MAC has a tight security reduction so has the IBE scheme. Furthermore, the transformation also extends to hierarchical identity-based encryption (HIBE). We also show how to construct affine MACs with a tight security reduction to standard assumptions. This, among other things, provides a tightly secure IBE in the standard model.

Keywords: IBE, HIBE, standard model, tight reduction

1 Introduction

Identity-based encryption (IBE) [28] enables a user to encrypt to a recipient's identity id (e.g., an email or phone number), and decryption can be done using a user secret key for id, obtained by a trusted authority. The first instantiations of an IBE scheme were given in 2001 [9, 6, 27]. Whereas earlier constructions relied on the random oracle model, the first adaptively secure construction in the standard model was proposed in [30]. Here adaptive security means that an adversary may select the challenge identity id^* after seeing the public key and arbitrarily many user secret keys for identities of his choice. The concept of IBE generalizes naturally to hierarchical IBE (HIBE). In an L-level HIBE, hierarchical identities are vectors of identities of maximal length L and user secret keys for a hierarchical identity can be delegated. An IBE is simply a L-level HIBE with $L = 1$.

In this work we focus on adaptively secure (H)IBE schemes in the standard model. The construction from [30] has the disadvantage of a non-tight security reduction, i.e., the security reduction reducing security of the L-level HIBE to the hardness of the underlying assumption loses at least a factor of Q^L, where Q is the maximal number of user secret key queries. Modern HIBE schemes [29, 8] only lose a factor Q, independent of L. The first tightly secure IBE was recently proposed by Chen and Wee [8] but designing a L-level HIBE for $L > 1$ and a tight (i.e., independent of Q) security reduction to a standard assumption remains an open problem.

Until now, all known constructions of (H)IBE schemes are specific, i.e., they are custom-made to a specific hardness assumption. This is in contrast to other basic cryptographic primitives such as signatures and public-key encryption, for which efficient generic transformations have been known for a long time. We would like to highlight the concept of smooth projective hash proof systems for chosen-ciphertext secure encryption [11] and an old construction by Bellare and Goldwasser [2] that transforms any pseudorandom function (PRF) plus a non-interactive zero-knowledge (NIZK) proof into a signature scheme. Until today no generic construction of a (H)IBE from any "simple" low-level cryptographic primitive is known. However, the recent IBE scheme by Chen and Wee [8] uses a specific randomized PRF at the core of their construction, but its usage is non-modular.

1.1 This Work

Affine MACs. In this work we put forward the notion of *affine message authentication codes* (affine MACs). An affine MAC over $\mathbb{Z}_q^n$ is a (randomized) MAC with a special algebraic structure over some group $\mathbb{G} = \langle g \rangle$ of prime-order q. For a vector $\mathbf{a} \in \mathbb{Z}_q^n$, define $[\mathbf{a}] := \mathbf{a}\mathcal{P} = (\mathbf{a}_1\mathcal{P}, \ldots, \mathbf{a}_n\mathcal{P})^\top \in \mathbb{G}^n$ as the implicit representation of $\mathbf{a}$ over $\mathbb{G}$. Roughly speaking, the MAC tag $\tau_{\mathsf{m}} = ([\mathbf{t}], [u])$ of an affine MAC over $\mathbb{Z}_q^n$ on message $\mathsf{m} \in \mathcal{M}$ is split into a random message-independent part $[\mathbf{t}] \in \mathbb{G}^n$ plus a message-depending affine part $[u] \in \mathbb{G}$ satisfying

$$u = \sum f_i(\mathsf{m})\mathbf{x}_i^\top \cdot \mathbf{t} + \sum f_i'(\mathsf{m})x_i' \in \mathbb{Z}_q, \tag{1}$$

where $f_i, f_i' : \mathcal{M} \to \mathbb{Z}_q$ are public functions and $\mathbf{x}_i \in \mathbb{Z}_q^n$, $x_i' \in \mathbb{Z}_q$ are from the secret key $\mathsf{sk}_{\mathsf{MAC}}$. Almost all group-based MACs recently considered in [12], as well as the MAC derived from the randomized Naor-Reingold PRF [25] implicitly given in [8] are affine.

From Affine MACs to (H)IBE. Let us fix (possibly symmetric) pairing groups $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ equipped with a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. Let $\mathcal{D}_k$-MDDH be any Matrix Diffie-Hellman Assumption [13]* that holds in $\mathbb{G}_1$, e.g., k-Linear or DDH.

Our main result is a *generic transformation* $\mathsf{IBE}[\mathsf{MAC}_n, \mathcal{D}_k]$ from any affine message authentication code MAC_n over $\mathbb{Z}_q^n$ into an IBE scheme. If MAC_n (defined over $\mathbb{G}_2$) is PR-CMA-secure (pseudorandom against chosen message attacks, a decisional variant of the standard UF-CMA security for MACs) and the $\mathcal{D}_k$-MDDH assumption holds in $\mathbb{G}_1$, then $\mathsf{IBE}[\mathsf{MAC}_n, \mathcal{D}_k]$ is an adaptively secure (and anonymous) IBE scheme. Furthermore, the security reduction of $\mathsf{IBE}[\mathsf{MAC}_n, \mathcal{D}_k]$ is as tight as the one of MAC_n. The size of the public IBE parameters depends on the size of the MAC secret key $\mathsf{sk}_{\mathsf{MAC}}$, whereas the IBE ciphertexts and user secret keys always contain $n + k + 1$ group elements. We stress that our transformation works with any $k \geq 1$ and any $\mathcal{D}_k$-MDDH Assumption, hence $\mathcal{D}_k$ can be chosen to match the security assumption of MAC_n.

We also extend our generic transformation to HIBE schemes. In particular, we have two generic HIBE constructions depending on different properties of the underlying affine MACs. If the affine MAC is *delegatable* (to be defined in Section 5.1), we obtain an adaptively secure L-level HIBE $\mathsf{HIBE}[\mathsf{MAC}_n, \mathcal{D}_k]$. Furthermore, if the affine MAC is delegatable and *anonymity-preserving* (to be defined in Section 5.5), we obtain an *anonymous* and adaptively secure L-level HIBE $\mathsf{AHIBE}[\mathsf{MAC}_n, \mathcal{D}_k]$. Both of the constructions have the same tightness properties as the MAC, and their ciphertexts sizes are the same as in the IBE case. Due to different delegation methods, $\mathsf{AHIBE}[\mathsf{MAC}_n, \mathcal{D}_k]$ has slightly shorter public parameters, but larger user secret keys than $\mathsf{HIBE}[\mathsf{MAC}_n, \mathcal{D}_k]$.

Let us highlight again the fact that the underlying object is a *symmetric* primitive (a MAC) that we transform to an *asymmetric* primitive (an IBE scheme). Furthermore, as a MAC is a very simple and well-understood object, we hope that our transformation can contribute to understanding the more complex object of an IBE scheme.

Two Constructions of Affine MAC. To instantiate our transformations, we consider two specific affine MACs. Our first construction, $\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k]$, is a generalization of the MAC derived from the affine Naor-Reingold PRF [8] to any $\mathcal{D}_k$-MDDH Assumption. (Unfortunately, the MAC based on the original deterministic Naor-Reingold PRF [25] is not affine.) We show that it is affine over $\mathbb{Z}_q^n$ with $n = k$. We prove its PR-CMA-security with an (almost) tight security reduction to $\mathcal{D}_k$-MDDH. (Almost tight, as the security reduction loses a factor $O(m)$, where m is the length of the message space.) This leads to a more efficient IBE (compared with [8]) with a tight security reduction to a standard assumption. Ciphertexts

*The $\mathcal{D}_k$-MDDH assumption over $\mathbb{G}_1$ captures naturally all subspace decisional assumptions over prime order groups. Concretely, it states that given $[\mathbf{A}]_1 \in \mathbb{G}^{(k+1)\times k}$, the value $[\mathbf{A} \cdot \mathbf{w}]_1 \in \mathbb{G}_1^{k+1}$ is pseudorandom, where $\mathbf{A} \in \mathbb{Z}_q^{(k+1)\times k}$ gets chosen according to distribution $\mathcal{D}_k$ and $\mathbf{w} \in \mathbb{Z}_q^k$. Examples include k-Linear and DDH ($k = 1$).

Scheme	$\vert\mathsf{pk}\vert$	$\vert\mathsf{usk}\vert$	$\vert\mathsf{C}\vert$	Anon.	Loss	Assumption
Wat05 [30]	$(4+\lambda)\vert\mathbb{G}_1\vert$	$2\vert\mathbb{G}_2\vert$	$2\vert\mathbb{G}_1\vert$	–	$O(\lambda Q)$	DBDH
Wat09 [29]	$12\vert\mathbb{G}_1\vert+\vert\mathbb{G}_T\vert$	$8\vert\mathbb{G}_2\vert+\vert\mathbb{Z}_q\vert$	$9\vert\mathbb{G}_1\vert+\vert\mathbb{Z}_q\vert$	–	$O(Q)$	2-LIN
Lew12 [22]	$24\vert\mathbb{G}_1\vert+\vert\mathbb{G}_T\vert$	$6\vert\mathbb{G}_2\vert$	$6\vert\mathbb{G}_1\vert$	$\surd$	$O(Q)$	2-LIN
CLL$^+$12 [7]	$8\vert\mathbb{G}_1\vert+\vert\mathbb{G}_T\vert$	$4\vert\mathbb{G}_2\vert$	$4\vert\mathbb{G}_1\vert$	–	$O(Q)$	SXDH
JR13 [17]	$6\vert\mathbb{G}_1\vert+\vert\mathbb{G}_T\vert$	$5\vert\mathbb{G}_2\vert$	$3\vert\mathbb{G}_1\vert+\vert\mathbb{Z}_q\vert$	–	$O(Q)$	SXDH
CW13 [8]	$2k^2(2\lambda+1)\vert\mathbb{G}_1\vert+k\vert\mathbb{G}_T\vert$	$4k\vert\mathbb{G}_2\vert$	$4k\vert\mathbb{G}_1\vert$	–	$O(\lambda)$	k-LIN
$\mathsf{IBE}_{\mathsf{HPS}}$	$(3k^2+4k)\vert\mathbb{G}_1\vert$	$(2k+2)\vert\mathbb{G}_2\vert$	$(2k+2)\vert\mathbb{G}_1\vert$	$\surd$	$O(Q)$	k-LIN
$\mathsf{IBE}_{\mathsf{NR}}$	$(2\lambda k^2+2k)\vert\mathbb{G}_1\vert$	$(2k+1)\vert\mathbb{G}_2\vert$	$(2k+1)\vert\mathbb{G}_1\vert$	$\surd$	$O(\lambda)$	k-LIN
Wat05 [30]	$O(\lambda L)\vert\mathbb{G}_1\vert$	$O(\lambda L)\vert\mathbb{G}_2\vert$	$(1+L)\vert\mathbb{G}_1\vert$	–	$O(\lambda Q)^L$	DBDH
Wat09 [29]	$O(L)\vert\mathbb{G}_1\vert$	$O(L)(\vert\mathbb{G}_2\vert+\vert\mathbb{Z}_q\vert)$	$O(L)(\vert\mathbb{G}_1\vert+\vert\mathbb{Z}_q\vert)$	–	$O(Q)$	2-LIN
CW13 [8]	$O(Lk^2)(\vert\mathbb{G}_1\vert+\vert\mathbb{G}_2\vert)$	$O(Lk)\vert\mathbb{G}_2\vert$	$(2k+2)\vert\mathbb{G}_1\vert$	–	$O(Q)$	k-LIN
$\mathsf{HIBE}_{\mathsf{HPS}}$	$O(Lk^2)(\vert\mathbb{G}_1\vert+\vert\mathbb{G}_2\vert)$	$O(Lk)\vert\mathbb{G}_2\vert$	$(2k+2)\vert\mathbb{G}_1\vert$	–	$O(Q)$	k-LIN
$\mathsf{AHIBE}_{\mathsf{HPS}}$	$O(Lk^2)\vert\mathbb{G}_1\vert$	$O(Lk^2)\vert\mathbb{G}_2\vert$	$(2k+2)\vert\mathbb{G}_1\vert$	$\surd$	$O(Q)$	k-LIN

Table 1: Top: comparison between known adaptively secure IBEs with identity-space $\mathcal{ID}=\{0,1\}^\lambda$ in prime order groups from standard assumptions. We count the number of group elements in $\mathbb{G}_1,\mathbb{G}_2$, and $\mathbb{G}_T$. Q is the number of user secret key queries by the adversary. 'Anon.' stands for anonymity. Here $\mathsf{IBE}_{\mathsf{HPS}} := \mathsf{IBE}[\mathsf{MAC}_{\mathsf{HPS}}[\mathcal{D}_k], k\text{-}\mathsf{LIN}]$, $\mathsf{IBE}_{\mathsf{NR}} := \mathsf{IBE}[\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k], k\text{-}\mathsf{LIN}]$ are from this paper. Bottom: comparison of L-level HIBEs with identity-space $\mathcal{ID}=(\{0,1\}^\lambda)^L$. $\mathsf{HIBE}_{\mathsf{HPS}} := \mathsf{HIBE}[\mathsf{MAC}_{\mathsf{HPS}}[\mathcal{D}_k], k\text{-}\mathsf{LIN}]$ and $\mathsf{AHIBE}_{\mathsf{HPS}} := \mathsf{AHIBE}[\mathsf{MAC}_{\mathsf{HPS}}[\mathcal{D}_k], k\text{-}\mathsf{LIN}]$ are from this paper.

and user secret keys of $\mathsf{IBE}[\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k],\mathcal{D}_k]$ only contain $2k+1$ group elements which is 3 in case we use $k=1$ and the SXDH Assumption (i.e., DDH in $\mathbb{G}_1$ and $\mathbb{G}_2$). Interestingly, our SXDH-based IBE scheme (given explicitly in Appendix D) can be seen as a "two-copy version" of Waters' IBE [30] which does not have a tight security reduction. The disadvantage of $\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k]$ is that the public parameters of $\mathsf{IBE}[\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k],\mathcal{D}_k]$ are linear in the bit-size of the identity space.

Our second construction, $\mathsf{MAC}_{\mathsf{HPS}}[\mathcal{D}_k]$, is based on a hash proof system given in [13] for any $\mathcal{D}_k$-MDDH problem. A hash proof system is known to imply a UF-CMA-secure MAC [12]. We extend this result to PR-CMA-security, where the reduction loses a factor of Q, the number of MAC queries. Furthermore, $\mathsf{MAC}_{\mathsf{HPS}}[\mathcal{D}_k]$ is affine over $\mathbb{Z}_q^{k+1}$ (i.e., $n=k+1$) and delegatable. Whereas public parameters of the L-level HIBE $\mathsf{HIBE}[\mathsf{MAC}_{\mathsf{HPS}}[\mathcal{D}_k],\mathcal{D}_k]$ only depend on L, ciphertexts and user secret keys contain $2k+2$ group elements which is 4 in case of the SXDH assumption ($k=1$). We remark that the efficiency of $\mathsf{HIBE}[\mathsf{MAC}_{\mathsf{HPS}}[\mathcal{D}_k],\mathcal{D}_k]$ is roughly the same as a HIBE proposed in [8]. Additionally, we show $\mathsf{MAC}_{\mathsf{HPS}}[\mathcal{D}_k]$ is also anonymity-preserving, which implies an anonymous (but non-tight) HIBE, $\mathsf{AHIBE}[\mathsf{MAC}_{\mathsf{HPS}}[\mathcal{D}_k],\mathcal{D}_k]$.

Table 1 summarizes all known (H)IBE scheme and their parameters.

Extensions. In fact, our generic transformation even gives (hierarchical) ID-based hash proof system from any (delegatable) affine MAC and the $\mathcal{D}_k$-MDDH assumption. From an (H)ID-based hash proof system one readily obtains an IND-ID-CCA-secure (H)IBE [20]. Furthermore, any (H)IBE directly implies a (Hierarchical ID-based) signature scheme [14, 18]. The signature obtained from $\mathsf{IBE}[\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k],\mathcal{D}_k]$ has a tight security reduction. Even though it is not entirely structure preserving, it can still be used to obtain a constant-size IND-CCA-secure public-key encryption scheme with a tight security reduction in the multi-user and multi-challenge setting [16, 4].

Follow-up Work. Recently, our generic transformation (from an affine MAC to an IBE) has been extended to construct quasi-adaptive non-interactive zero-knowledge proof systems for linear subspaces [21] and (linearly homomorphic) structure-preserving signature schemes [21, 19].

1.2 Technical Details

Our Transformation. The high level idea behind our generic transformation $\mathsf{IBE}[\mathsf{MAC},\mathcal{D}_k]$ from any affine MAC over $\mathbb{Z}_q^n$ to an IBE scheme is the transformation from Bellare and Goldwasser [2] from a MAC (originally, a PRF) and a NIZK to a signature scheme. We use the same approach but define the user secret keys to be Bellare-Goldwasser signatures. The (H)IBE encryption functionality makes use of the special properties of the algebraic MAC and (tuned) Groth-Sahai proofs.

Concretely, the public key pk of the IBE scheme contains special perfectly hiding commitments $[\mathbf{Z}]_1$ to the MAC secret keys $\mathsf{sk}_{\mathsf{MAC}}$, which also depend on the $\mathcal{D}_k$-MDDH assumption. The user secret key $\mathsf{usk}[\mathsf{id}]$ of an identity id contains the MAC tag $\tau_{\mathsf{id}} = ([\mathbf{t}]_2, [u]_2) \in \mathbb{G}_2^{n+1}$ on id, plus a tuned Groth-Sahai [15] non-interactive zero-knowledge (NIZK) proof π that τ_{id} was computed correctly with respect to the commitments $[\mathbf{Z}]_1$ containing $\mathsf{sk}_{\mathsf{MAC}}$. Since the MAC is affine, the NIZK proof $\pi \in \mathbb{G}^k$ is very compact. The next observation is that the NIZK verification equation for π is a linear equation in the (committed) MAC secret keys and hence a randomized version of it gives rise to the IBE ciphertext and a decryption algorithm.

Security Proof. The security proof can also be sketched easily at a high level. We first apply a Cramer-Shoup argument [10], where we decrypt the IBE challenge ciphertext using the MAC secret key $\mathsf{sk}_{\mathsf{MAC}}$. Next, we make the challenge ciphertext inconsistent which involves one application of the $\mathcal{D}_k$-MDDH assumption. Now we can use the NIZK simulation routine to simulate the NIZK proof π from the user secret key $\mathsf{usk}[\mathsf{id}] = (\tau_{\mathsf{id}}, \pi)$. At this point, as the commitments perfectly hide the MAC secret keys $\mathsf{sk}_{\mathsf{MAC}}$, the only part of the security experiment still depending on $\mathsf{sk}_{\mathsf{MAC}}$ is τ_{id} from $\mathsf{usk}[\mathsf{id}]$ plus the computation of the challenge ciphertext. Now we are in the position to make the reduction to the symmetric primitive. We can use the PR-CMA symmetric security of MAC to argue directly about the pseudorandomness of the IBE challenge ciphertext. An IBE with pseudorandom ciphertexts is both IND-CPA secure and anonymous.

1.3 Other Related Work

Recently, Wee [31] proposed an information-theoretic primitive called *predicate encodings* that characterize the underlying algebraic structure of a number of predicate encoding schemes, including known IBE [24] and attribute-based encryption (ABE) [23] schemes. The main conceptual difference to affine MACs is that predicate encodings is a purely information-theoretic object. Furthermore, the framework by Wee is inherently limited to composite order groups.

Waters introduced the dual system framework [29] in order to facility tighter proofs for (H)IBE systems and beyond. The basic idea is that there exists functional and semi-functional ciphertexts and user secret keys, that are computationally indistinguishable. Decrypting a ciphertext with a user secret key is successful unless both are semi-functional. The $\mathcal{D}_k$-MDDH assumptions are specifically tailored to the dual system framework as they provide natural subspace assumptions over $\mathbb{G}^{k+1}$. Previous dual system constructions [29, 24, 8] usually first construct a scheme over composite-order groups and then transform it into prime-order groups. As the transformation uses a subspace assumption over $\mathbb{G}^{k+1}$ for *each component* of the composite-order group, ciphertexts and user secret keys contain at least $2(k+1)$ group elements. An exception is a recent *direct construction* in prime-order groups by Jutla and Roy [17]. Their scheme is based on the SXDH assumption (*i.e.*, $k = 1$) and achieves slightly better ciphertext size of 3 group elements plus one element from $\mathbb{Z}_q$. Even though our construction and proof strategy is inspired by the Bellare-Goldwasser NIZK approach and Cramer-Shoup's hash proof systems, we still roughly follow the dual system framework. However, as we give a direct construction in prime-order groups, our IBE scheme $\mathsf{IBE}[\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k], \mathcal{D}_k]$ has ciphertexts and user secret keys of size $2k+1$, breaking the "$2(k+1)$ barrier".

1.4 Open Problems

We leave finding a PR-CMA-secure algebraic MAC with a tight security reduction and constant-size secret keys as a main open problem. Given our main result this would directly imply a tightly-secure IBE with constant-size public parameters. Furthermore, we leave finding a tightly-secure (anonymity-preserving) delegatable affine MAC as an open problem, which would imply a tightly-secure (anonymous) HIBE.

Finally, we think that the concept of algebraic MACs can be extended such that our transformation also covers more general predicate encoding schemes, including attribute-based encryption.

1.5 Publication Info

An extended abstract of this work appeared in the proceedings of CRYPTO 2014 [5]. Theorem 4 of [5] claimed that $\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k]$ is a tightly-secure delegatable affine MAC (implying a tightly-secure HIBE by our transformation in Section 5.4). We removed this theorem because its proof contained a flaw. This was pointed out by Jie Chen.

2 Definitions

2.1 Notation

If $\mathbf{x} \in \mathcal{B}^n$, then $|\mathbf{x}|$ denotes the length n of the vector. Further, $x \stackrel{\$}{\leftarrow} \mathcal{B}$ denotes the process of sampling an element x from set $\mathcal{B}$ uniformly at random. If $\mathbf{A} \in Z_q^{(k+1)\times n}$ is a matrix, then $\overline{\mathbf{A}} \in \mathbb{Z}_q^{k\times n}$ denotes the upper matrix of $\mathbf{A}$ and then $\underline{\mathbf{A}} \in \mathbb{Z}_q^{1\times k}$ denotes the last row of $\mathbf{A}$.

Games. We use games for our security reductions. A game G is defined by procedures Initialize and Finalize, plus some optional procedures $\mathrm{P}_1, \ldots, \mathrm{P}_n$. All procedures are given using pseudo-code, where initially all variables are undefined. An adversary $\mathcal{A}$ is executed in game G if it first calls Initialize, obtaining its output. Next, it may make arbitrary queries to P_i (according to their specification), again obtaining their output. Finally, it makes one single call to Finalize$(\cdot)$ and stops. We define $\mathsf{G}^{\mathcal{A}}$ as the output of $\mathcal{A}$'s call to Finalize.

2.2 Pairing groups and Matrix Diffie-Hellman Assumption

Let GGen be a probabilistic polynomial time (PPT) algorithm that on input 1^λ returns a description $\mathcal{G} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, \mathcal{P}_1, \mathcal{P}_2, e)$ of asymmetric pairing groups where $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$ are cyclic groups of order q for a λ-bit prime q, $\mathcal{P}_1$ and $\mathcal{P}_2$ are generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively, and $e : \mathbb{G}_1 \times \mathbb{G}_2$ is an efficiently computable (non-degenerated) bilinear map. Define $\mathcal{P}_T := e(\mathcal{P}_1, \mathcal{P}_2)$, which is a generator in $\mathbb{G}_T$.

We use implicit representation of group elements as introduced in [13]. For $s \in \{1, 2, T\}$ and $a \in \mathbb{Z}_q$ define $[a]_s = a\mathcal{P}_s \in \mathbb{G}_s$ as the *implicit representation* of a in $\mathbb{G}_s$. More generally, 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 $\mathbb{G}_s$:

$$[\mathbf{A}]_s := \begin{pmatrix} a_{11}\mathcal{P}_s & \ldots & a_{1m}\mathcal{P}_s \\ \\ a_{n1}\mathcal{P}_s & \ldots & a_{nm}\mathcal{P}_s \end{pmatrix} \in \mathbb{G}_s^{n\times m}$$

We will always use this implicit notation of elements in $\mathbb{G}_s$, i.e., we let $[a]_s \in \mathbb{G}_s$ be an element in $\mathbb{G}_s$. Note that from $[a]_s \in \mathbb{G}_s$ it is generally hard to compute the value a (discrete logarithm problem in $\mathbb{G}_s$). Further, from $[b]_T \in \mathbb{G}_T$ it is hard to compute the value $[b]_1 \in \mathbb{G}_1$ and $[b]_2 \in \mathbb{G}_2$ (pairing inversion problem). Obviously, given $[a]_s \in \mathbb{G}_s$ and a scalar $x \in \mathbb{Z}_q$, one can efficiently compute $[ax]_s \in \mathbb{G}_s$. Further, given $[a]_1, [a]_2$ one can efficiently compute $[ab]_T$ using the pairing e. For $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_q^k$ define $e([\mathbf{a}]_1, [\mathbf{b}]_2) := [\mathbf{a}^\top \mathbf{b}]_T \in \mathbb{G}_T$.

We recall the definition of the matrix Diffie-Hellman (MDDH) assumption [13].

Definition 2.1 (Matrix Distribution) *Let $k \in \mathbb{N}$. We call $\mathcal{D}_k$ a matrix distribution if it outputs matrices in $\mathbb{Z}_q^{(k+1)\times k}$ of full rank k in polynomial time.*

Without loss of generality, we assume the first k rows of $\mathbf{A} \stackrel{\$}{\leftarrow} \mathcal{D}_k$ form an invertible matrix. The $\mathcal{D}_k$-Matrix Diffie-Hellman problem is to distinguish the two distributions $([\mathbf{A}], [\mathbf{Aw}])$ and $([\mathbf{A}], [\mathbf{u}])$ where $\mathbf{A} \stackrel{\$}{\leftarrow} \mathcal{D}_k$, $\mathbf{w} \stackrel{\$}{\leftarrow} \mathbb{Z}_q^k$ and $\mathbf{u} \stackrel{\$}{\leftarrow} \mathbb{Z}_q^{k+1}$.

Definition 2.2 ($\mathcal{D}_k$-Matrix Diffie-Hellman Assumption $\mathcal{D}_k$-MDDH) *Let $\mathcal{D}_k$ be a matrix distribution and $s \in \{1, 2, T\}$. We say that the $\mathcal{D}_k$-Matrix Diffie-Hellman ($\mathcal{D}_k$-MDDH) Assumption holds relative to GGen in group $\mathbb{G}_s$ if for all PPT adversaries $\mathcal{D}$,*

$$\mathbf{Adv}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{D}) := |\Pr[\mathcal{D}(\mathcal{G}, [\mathbf{A}]_s, [\mathbf{Aw}]_s) = 1] - \Pr[\mathcal{D}(\mathcal{G}, [\mathbf{A}]_s, [\mathbf{u}]_s) = 1]| = negl(\lambda),$$

where the probability is taken over $\mathcal{G} \stackrel{\$}{\leftarrow} \mathsf{GGen}(1^\lambda)$, $\mathbf{A} \stackrel{\$}{\leftarrow} \mathcal{D}_k, \mathbf{w} \stackrel{\$}{\leftarrow} \mathbb{Z}_q^k, \mathbf{u} \stackrel{\$}{\leftarrow} \mathbb{Z}_q^{k+1}$.

For each $k \geq 1$, [13] specifies distributions $\mathcal{L}_k$, $\mathcal{C}_k$, $\mathcal{SC}_k$, $\mathcal{IL}_k$ such that the corresponding $\mathcal{D}_k$-MDDH assumption is the k-Linear assumption, the k-Cascade, the k-Symmetric Cascade, and the Incremental k-Linear Assumption, respectively. All assumptions are generically secure in bilinear groups and form a hierarchy of increasingly weaker assumptions. The distributions are exemplified for $k = 2$, where $a_1, \ldots, a_6 \xleftarrow{\$} \mathbb{Z}_q$.

$$\mathcal{C}_2 : \mathbf{A} = \begin{pmatrix} a_1 & 0 \\ 1 & a_2 \\ 0 & 1 \end{pmatrix} \quad \mathcal{SC}_2 : \mathbf{A} = \begin{pmatrix} a_1 & 0 \\ 1 & a_1 \\ 0 & 1 \end{pmatrix} \quad \mathcal{L}_2 : \mathbf{A} = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \\ 1 & 1 \end{pmatrix} \quad \mathcal{U}_2 : \mathbf{A} = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \\ a_5 & a_6 \end{pmatrix}.$$

It was also shown in [13] that $\mathcal{U}_k$-MDDH is implied by all other $\mathcal{D}_k$-MDDH assumptions. If $\mathbf{A}$ is chosen from $\mathcal{SC}_k$, then $[\mathbf{A}]_s$ can be represented with 1 group element; if $\mathbf{A}$ is chosen from $\mathcal{L}_k$ or $\mathcal{C}_k$, then $[\mathbf{A}]_s$ can be represented with k group elements; If $\mathbf{A}$ is chosen from $\mathcal{U}_k$, then $[\mathbf{A}]_s$ can be represented with $(k+1)k$ group elements. Hence, $\mathcal{SC}_k$-MDDH offers the same security guarantees as k-Linear, while having the advantage of a more compact representation.

Let $m \geq 1$. For $\mathbf{W} \xleftarrow{\$} \mathbb{Z}_q^{k \times m}, \mathbf{U} \xleftarrow{\$} \mathbb{Z}_q^{(k+1) \times m}$, consider the m-fold $\mathcal{D}_k$-MDDH problem which is distinguishing the distributions $([\mathbf{A}], [\mathbf{AW}])$ and $([\mathbf{A}], [\mathbf{U}])$. That is, the m-fold $\mathcal{D}_k$-MDDH problem contains m independent instances of the $\mathcal{D}_k$-MDDH problem (with the same $\mathbf{A}$ but different $\mathbf{w}_i$). By a hybrid argument one can show that the two problems are equivalent, where the reduction loses a factor m. The following lemma gives a tight reduction.

Lemma 2.3 (Random self reducibility [13]) *For any matrix distribution $\mathcal{D}_k$, $\mathcal{D}_k$-MDDH is random self-reducible. In particular, for any $m \geq 1$,*

$$\mathbf{Adv}_{\mathcal{D}_k, \mathsf{GGen}}(\mathcal{D}) + \frac{1}{q-1} \geq \mathbf{Adv}^m_{\mathcal{D}_k, \mathsf{GGen}}(\mathcal{D}') := \Pr[\mathcal{D}'(\mathcal{G}, [\mathbf{A}], [\mathbf{AW}]) \Rightarrow 1] - \Pr[\mathcal{D}'(\mathcal{G}, [\mathbf{A}], [\mathbf{U}]) \Rightarrow 1],$$

with $\mathcal{G} \leftarrow \mathsf{GGen}(1^\lambda)$, $\mathbf{A} \xleftarrow{\$} \mathcal{D}_k, \mathbf{W} \xleftarrow{\$} \mathbb{Z}_q^{k \times m}, \mathbf{U} \xleftarrow{\$} \mathbb{Z}_q^{(k+1) \times m}$.

3 Message Authentication Codes

We use the standard definition of a (randomized) message authentication code $\mathsf{MAC} = (\mathsf{Gen}_{\mathsf{MAC}}, \mathsf{Tag}, \mathsf{Ver})$, where $\mathsf{sk}_{\mathsf{MAC}} \xleftarrow{\$} \mathsf{Gen}_{\mathsf{MAC}}(\mathsf{par})$ returns a secret key, $\tau \xleftarrow{\$} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m})$ returns a tag τ on message m from some message space $\mathcal{M}$, and $\mathsf{Ver}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m}, \tau) \in \{0, 1\}$ returns a verification bit.

3.1 Affine MACs

Affine MACs over $\mathbb{Z}_q^n$ are group-based MACs with a specific algebraic structure.

Definition 3.1 *Let* par *be system parameters containing a group $\mathcal{G} = (\mathbb{G}_2, q, g_2)$ of prime-order q and let $n \in \mathbb{N}$. We say that* $\mathsf{MAC} = (\mathsf{Gen}_{\mathsf{MAC}}, \mathsf{Tag}, \mathsf{Ver})$ *is* affine over $\mathbb{Z}_q^n$ *if the following conditions hold:*

1. $\mathsf{Gen}_{\mathsf{MAC}}(\mathsf{par})$ *returns* $\mathsf{sk}_{\mathsf{MAC}}$ *containing $(\mathbf{B}, \mathbf{x}_0, \ldots, \mathbf{x}_\ell, x'_0, \ldots, x'_{\ell'})$, where $\mathbf{B} \in \mathbb{Z}_q^{n \times n'}$, $\mathbf{x}_i \in \mathbb{Z}_q^n$, $x'_j \in \mathbb{Z}_q$, for some $n', \ell, \ell' \in \mathbb{N}$. We assume $\mathbf{B}$ has rank at least one.*
2. $\mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m} \in \mathcal{B}^\ell)$ *returns a tag $\tau = ([\mathbf{t}]_2, [u]_2) \in \mathbb{G}_2^n \times \mathbb{G}_2$, computed as*

$$\mathbf{t} \;=\; \mathbf{Bs} \in \mathbb{Z}_q^n \qquad \text{for } \mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^{n'} \tag{2}$$

$$u \;=\; \sum_{i=0}^{\ell} f_i(\mathsf{m}) \mathbf{x}_i^\top \mathbf{t} + \sum_{i=0}^{\ell'} f'_i(\mathsf{m}) x'_i \in \mathbb{Z}_q \tag{3}$$

   for some public defining functions *$f_i : \mathcal{M} \to \mathbb{Z}_q$ and $f'_i : \mathcal{M} \to \mathbb{Z}_q$. Vector $\mathbf{s}$ can be generated either pseudorandomly (cf.* $\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k]$*) or randomly (cf.* $\mathsf{MAC}_{\mathsf{HPS}}[\mathcal{D}_k]$*) and u is the (deterministic) message-depending part.*
3. $\mathsf{Ver}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m}, \tau = ([\mathbf{t}]_2, [u]_2))$ *verifies if equation (3) holds.*

<u>INITIALIZE:</u> $\mathsf{sk_{MAC}} \xleftarrow{\$} \mathsf{Gen_{MAC}}(\mathsf{par})$ Return ε <u>EVAL(m):</u> $\mathcal{Q_M} = \mathcal{Q_M} \cup \{\mathsf{m}\}$ Return $([\mathbf{t}]_2, [u]_2) \xleftarrow{\$} \mathsf{Tag}(\mathsf{sk_{MAC}}, \mathsf{m})$	<u>CHAL(m^*):</u> //one query $h \xleftarrow{\$} \mathbb{Z}_q^*$ $\mathbf{h}_0 = \sum f_i(\mathsf{m}^*)\mathbf{x}_i \cdot h \in \mathbb{Z}_q^n$; $h_1 = \sum f'_i(\mathsf{m}^*)x'_i \cdot h \in \mathbb{Z}_q$ $\boxed{\mathbf{h}_0 \xleftarrow{\$} \mathbb{Z}_q^n;\ h_1 \xleftarrow{\$} \mathbb{Z}_q}$ Return $([h]_1, [\mathbf{h}_0]_1, [h_1]_T)$ <u>FINALIZE($d \in \{0,1\}$):</u> Return $d \wedge (\mathsf{m}^* \notin \mathcal{Q_M})$

Figure 1: Games $\mathsf{PR\text{-}CMA_{real}}$ and $\boxed{\mathsf{PR\text{-}CMA_{rand}}}$ for defining PR-CMA security. In all procedures, the boxed statements redefining $(\mathbf{h}_0, h_1)$ are only executed in game $\mathsf{PR\text{-}CMA_{rand}}$.

The standard security notion for probabilistic MACs is unforgeability against chosen-message attacks UF-CMA [12]. In this work we require *pseudorandomness against chosen-message attacks* (PR-CMA), which is slightly stronger than UF-CMA. Essentially, we require that the values used for one single verification equation (3) on message m^* are pseudorandom over $\mathbb{G}_1$ and $\mathbb{G}_T$.

Let $\mathcal{G} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, g_1, g_2, e)$ be an asymmetric pairing group such that $(\mathbb{G}_2, g_2, q)$ is contained in par. We define the PR-CMA security via games $\mathsf{PR\text{-}CMA_{real}}$ and $\mathsf{PR\text{-}CMA_{rand}}$ from Figure 1. Note that the output $([h]_1, [\mathbf{h}_0]_1, [h_1]_T)$ of CHAL(m^*) in game $\mathsf{PR\text{-}CMA_{real}}$ can be viewed as a "token" for message m^* to check verification equation (3) for arbitrary tags $([\mathbf{t}]_2, [u]_2)$ via equation $e([h]_1, [u]_2) \stackrel{?}{=} e([\mathbf{t}]_1, [\mathbf{h}_0]_1) \cdot [h_1]_T$. Intuitively, the pseudorandomness of $[h_1]_T$ is responsible for indistinguishabilty and of $[\mathbf{h}_0]_1$ to prove anonymity of the IBE scheme.

Definition 3.2 *An affine* MAC *over* $\mathbb{Z}_q^n$ *is* PR-CMA*-secure if for all PPT* $\mathcal{A}$, $\mathsf{Adv}^{\mathsf{pr\text{-}cma}}_{\mathsf{MAC}}(\mathcal{A}) := \Pr[\mathsf{PR\text{-}CMA}^{\mathcal{A}}_{\mathsf{real}} \Rightarrow 1] - \Pr[\mathsf{PR\text{-}CMA}^{\mathcal{A}}_{\mathsf{rand}} \Rightarrow 1]$ *is negligible, where the experiments are defined in Figure 1.*

3.2 An Affine MAC from the Naor-Reingold PRF

Unfortunately, the (deterministic) Naor-Reingold pseudorandom function is not affine. Let $\mathsf{PRF} : \mathcal{M} \to \mathbb{Z}_q^k$ be a pseudorandom function and we use the following randomized version $\mathsf{MAC_{NR}}[\mathcal{D}_k] = (\mathsf{Gen_{MAC}}, \mathsf{Tag}, \mathsf{Ver})$ of it based on any matrix assumption $\mathcal{D}_k$. For the special case $\mathcal{D}_k = \mathcal{L}_k$, it was implicitly given in [8]. Recall that, for any matrix $\mathbf{A} \in \mathbb{Z}_q^{(k+1)\times k}$ we denote the upper k rows by $\overline{\mathbf{A}} \in \mathbb{Z}_q^{k\times k}$ and the last row by $\underline{\mathbf{A}} \in \mathbb{Z}_q^{1\times k}$.

<u>$\mathsf{Gen_{MAC}}(\mathsf{par})$:</u> $\mathbf{A} \xleftarrow{\$} \mathcal{D}_k$; $\mathbf{B} := \overline{\mathbf{A}} \in \mathbb{Z}_q^{k\times k}$ $\mathbf{x}_{1,0}, \dots, \mathbf{x}_{m,1} \xleftarrow{\$} \mathbb{Z}_q^k$; $x'_0 \xleftarrow{\$} \mathbb{Z}_q$ $\mathsf{sk_{MAC}} = (\mathbf{B}, \mathbf{x}_{1,0}, \dots, \mathbf{x}_{m,1}, x'_0)$ Return $\mathsf{sk_{MAC}}$	<u>$\mathsf{Tag}(\mathsf{sk_{MAC}}, \mathsf{m})$:</u> $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k, \mathbf{t} = \mathbf{B}\mathbf{s}$ $u = (\sum_{i=1}^{\lvert\mathsf{m}\rvert} \mathbf{x}_{i,\mathsf{m}_i}^\top)\mathbf{t} + x'_0 \in \mathbb{Z}_q$ Return $\tau = ([\mathbf{t}]_2, [u]_2) \in \mathbb{G}_2^k \times \mathbb{G}_2$	<u>$\mathsf{Ver}(\mathsf{sk_{MAC}}, \tau, \mathsf{m})$:</u> If $u = (\sum_{i=1}^{\lvert\mathsf{m}\rvert} \mathbf{x}_{i,\mathsf{m}_i}^\top)\mathbf{t} + x'_0$ then return 1; Else return 0.

Note that $\mathsf{MAC_{NR}}[\mathcal{D}_k]$ is n-affine over $\mathbb{Z}_q^n$ with message space $\mathcal{M} = \{0,1\}^m$. Writing $\mathbf{x}_{i,b} = \mathbf{x}_{2i+b}$ we have $n = n' = k$, $\ell' = 0$, $\ell = 2m+1$ and functions $f_0(\mathsf{m}) = f_1(\mathsf{m}) = 0$, $f'_0(\mathsf{m}) = 1$, and $f_{2i+b}(\mathsf{m}) = (\mathsf{m}_i = b)$ for $1 \le i \le m$. (To perfectly fit our definition, $\mathbf{x}_{i,b}$ should be renamed to $\mathbf{x}_{2i+b}$, but we conserve the other notations for better readability.)

We show $\mathsf{MAC_{NR}}[\mathcal{D}_k]$ satisfies a weaker version of PR-CMA security, called $\mathsf{PR\text{-}CMA_0}$ security, where an adversary is allowed to query EVAL on each message m at most once. $\mathsf{PR\text{-}CMA_0}$ can be converted to PR-CMA security by generating $\mathbf{s}$ using a pseudo-random function PRF on m such that Tag is deterministic.

Theorem 3.3 $\mathsf{MAC_{NR}}[\mathcal{D}_k]$ *is tightly* $\mathsf{PR\text{-}CMA_0}$*-secure under the* $\mathcal{D}_k$-MDDH *assumption. In particular, for all adversaries* $\mathcal{A}$ *there exist adversaries* $\mathcal{B}_1$ *with* $\mathbf{T}(\mathcal{B}_1) \approx \mathbf{T}(\mathcal{A})$ *and*

$$\mathsf{Adv}^{\mathsf{pr\text{-}cma_0}}_{\mathsf{MAC_{NR}}[\mathcal{D}_k]}(\mathcal{A}) \le 4m(\mathbf{Adv}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}_1) - 1/(q-1)).$$

Initialize: // Games G_0, $\boxed{\mathsf{G}_{1,i}, \mathsf{G}_2}$
$\mathbf{A} \xleftarrow{\$} \mathcal{D}_k$
For $j = 1, \ldots, m : \mathbf{x}_{j,0}, \mathbf{x}_{j,1} \leftarrow \mathbb{Z}_q^k$
$x'_0 \leftarrow_{\$} \mathbb{Z}_q$; $\boxed{x'_0 \text{ is undefined}}$
Return ε

Chal(m^*): // Games G_0, $\boxed{\mathsf{G}_{1,i}}$, $\boxed{\mathsf{G}_2}$, one query
$h \xleftarrow{\$} \mathbb{Z}_q$; $\boxed{x'_0 = \mathsf{RF}_i(\mathsf{m}^*_{|i})}$
$\mathbf{h}_0 = (\sum_{j=1}^{m} \mathbf{x}_{j,\mathsf{m}^*_j}) \cdot h$; $h_1 = x'_0 \cdot h \in \mathbb{Z}_q$
$\boxed{\mathbf{h}_0 \xleftarrow{\$} \mathbb{Z}_q^k;\ h_1 \xleftarrow{\$} \mathbb{Z}_q}$
Return $([h]_1, [\mathbf{h}_0]_1, [h_1]_T)$

Eval(m): // Games G_0, $\boxed{\mathsf{G}_{1,i}}$, $\boxed{\mathsf{G}_2}$
$\mathcal{Q}_{\mathcal{M}} = \mathcal{Q}_{\mathcal{M}} \cup \{\mathsf{m}\}$
$\mathbf{s}_\mathsf{m} \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{t}_\mathsf{m} = \mathbf{B}\mathbf{s}_\mathsf{m}$
$u_\mathsf{m} = \sum_{j=1}^{m} \mathbf{x}_{j,\mathsf{m}_j}^\top \mathbf{t}_\mathsf{m} + x'_0$
$\boxed{u_\mathsf{m} = \sum_{j=1}^{m} \mathbf{x}_{j,\mathsf{m}_j}^\top \mathbf{t}_\mathsf{m} + \mathsf{RF}_i(\mathsf{m}_{|i})}$
$\boxed{u_\mathsf{m} \xleftarrow{\$} \mathbb{Z}_q}$
Return $([\mathbf{t}_\mathsf{m}]_2, [u_\mathsf{m}]_2)$

Finalize($d \in \{0,1\}$): // Games G_0-G_2
Return $d \wedge (\mathsf{m}^* \notin \mathcal{Q}_{\mathcal{M}})$

Figure 2: Games G_0, G_1 and $\mathsf{G}_{2,i}$ $(0 \leq i \leq m)$ for the proof of Lemmas 3.4 to 3.7. $\mathsf{RF}_i : \{0,1\}^i \to \mathbb{Z}_q$ is a random function and $\mathsf{m}_{|i}$ denotes the ith prefix of m. In each procedure, a solid (dotted) frame indicates that the command is only executed in the game marked by a solid (dotted) frame.

Note that the security bound is (almost) tight, as m is the bit-length of message space $\mathcal{M}$. The proof follows the ideas from [8, 26]. We use m hybrids, where in hybrid i *all* the (maximal Q) values $\mathbf{x}_{i,1-\mathsf{m}^*_i}^\top \cdot \mathbf{t}$ in the response to an Eval query are replaced by uniform randomness. Here m^* is the message from the challenge query. We use the Q-fold $\mathcal{D}_k$-MDDH assumption to interpolate between the hybrids, where the reductions guesses m^*_i correctly with probability 1/2. As the Q-fold $\mathcal{D}_k$-MDDH assumption is tightly implied by the standard $\mathcal{D}_k$-MDDH assumption (Lemma 2.3), the proof follows.

We remark, that one can define an alternative version of $\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k]$ by setting $\mathbf{x}_0 := \sum \mathbf{x}_{i,0}$, $\mathbf{x}_i := \mathbf{x}_{i,1} - \mathbf{x}_{i,0}$ and $u = (\mathbf{x}_0^\top + \sum_{i=1}^{|\mathsf{m}|} \mathsf{m}_i \mathbf{x}_i^\top)\mathbf{t} + x'_0$. This MAC has a shorter secret key and can also be shown to be PR-CMA. (However, it does not satisfy the stronger security notion of HPR-CMA needed in Section 5.)

Proof of Theorem 3.3: Let $\mathcal{A}$ be an adversary against the PR-CMA-security of $\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k]$. We prove Theorem 3.3 by defining a sequence of intermediate games as in Figure 2 and 4.

Game G_0 is the real attack game.

Lemma 3.4 $\Pr[\mathsf{PR\text{-}CMA}_{\mathsf{real}}^{\mathcal{A}} \Rightarrow 1] = \Pr[\mathsf{G}_0^{\mathcal{A}} \Rightarrow 1]$.

In $\mathsf{G}_{1,0}$, we syntactically replace x'_0 by $\mathsf{RF}_0(\epsilon)$ which is a fixed random element.

Lemma 3.5 $\Pr[\mathsf{G}_0^{\mathcal{A}} \Rightarrow 1] = \Pr[\mathsf{G}_{1,0}^{\mathcal{A}} \Rightarrow 1]$.

Lemma 3.6 *There exists an adversary* $\mathcal{B}_1$ *with* $\mathbf{T}(\mathcal{B}_1) \approx \mathbf{T}(\mathcal{A})$ *and* $|\Pr[\mathsf{G}_{1,i}^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathsf{G}_{1,i-1}^{\mathcal{A}} \Rightarrow 1]| \leq 2(\mathbf{Adv}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}_1) - \frac{1}{q-1})$.

Proof: Let Q be the maximal number of Eval queries made by $\mathcal{A}$. We first build an adversary $\mathcal{B}'$ against the Q-fold $\mathcal{D}_k$-MDDH Assumption such that

$$2\mathbf{Adv}^{Q}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}') \geq |\Pr[\mathsf{G}_{1,i}^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathsf{G}_{1,i-1}^{\mathcal{A}} \Rightarrow 1]|. \tag{4}$$

This implies the lemma using the random self reducibility of the MDDH assumption (Lemma 2.3).

On input of a Q-fold $\mathcal{D}_k$-MDDH challenge $([\mathbf{A}]_2, [\mathbf{H}]_2) \in \mathbb{G}_2^{(k+1)\times k} \times \mathbb{G}_2^{(k+1)\times Q}$, $\mathcal{B}'$ first picks a random bit b which is a guess for m^*_i. Let RF_{i-1} and RF'_{i-1} be two independent random functions (defined on the fly) which we use to define

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

<u>INITIALIZE:</u> $b \xleftarrow{\$} \{0,1\}$ For $j = 1,\dots,m$ and $j' = 0,1$: If $j \neq i$ or $j' = b$ then $\mathbf{x}_{j,j'} \xleftarrow{\$} \mathbb{Z}_q^k$ $\mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^{k+1}$; $\mathbf{x}_{i,1-b}^\top \overline{\mathbf{A}} := \mathbf{r}^\top \mathbf{A} \in \mathbb{Z}_q^k$ Return ε <u>CHAL(m^*):</u> Abort if $\mathsf{m}^*_i \neq b$. $h \xleftarrow{\$} \mathbb{Z}_q$; $x_0' = \mathsf{RF}_{i-1}(\mathsf{m}^*_{\vert i-1})$ $\mathbf{h}_0 = (\sum_{j=1}^m \mathbf{x}_{j,\mathsf{m}^*_j}) h \in \mathbb{Z}_q^k$ $h_1 = x_0' h \in \mathbb{Z}_q$ Return $([h]_1, [\mathbf{h}_0]_1, [h_1]_T)$	<u>EVAL(m):</u> $\mathcal{Q}_\mathcal{M} = \mathcal{Q}_\mathcal{M} \cup \{\mathsf{m}\}$ $c := \alpha_i(\mathsf{m}_{\vert i})$ $\mathbf{s}'_\mathsf{m} \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{t}_\mathsf{m} = \overline{\mathbf{A}}\mathbf{s}'_\mathsf{m} + \overline{\mathbf{H}}_c$ $u_\mathsf{m} = \begin{cases} (\sum_{j=1}^{\vert\mathsf{m}\vert} \mathbf{x}_{j,\mathsf{m}_j}^\top)\mathbf{t}_\mathsf{m} + \mathsf{RF}_{i-1}(\mathsf{m}_{\vert i-1}) & \mathsf{m}_i = b \\ (\sum_{j \neq i} \mathbf{x}_{j,\mathsf{m}_j}^\top)\mathbf{t}_\mathsf{m} + \mathbf{r}^\top(\mathbf{A}\mathbf{s}'_\mathsf{m} + \mathbf{H}_c) + \mathsf{RF}_{i-1}(\mathsf{m}_{\vert i-1}) & \mathsf{m}_i = 1-b \end{cases}$ Return $([\mathbf{t}_\mathsf{m}]_2, [u_\mathsf{m}]_2)$ <u>FINALIZE($d \in \{0,1\}$):</u> Return $d \wedge (\mathsf{m}^* \notin \mathcal{Q}_\mathcal{M})$

Figure 3: Description of $\mathcal{B}'(\mathcal{G}, [\mathbf{A}]_2, [\mathbf{H}]_2)$ interpolating between the Games $\mathsf{G}_{1,i}$ and $\mathsf{G}_{1,i-1}$, where $\mathbf{H}_c$ denotes the c-th column of $\mathbf{H}$ and $\alpha_i : \{0,1\}^i \to \{1,\dots,Q\}$ is an injective function.

The construction of $\mathcal{B}'$ is described in Figure 3. Note that if RF_{i-1} and RF'_{i-1} are random functions, then RF_i is a random function.

Assume $\mathcal{B}'$ correctly guesses $b = \mathsf{m}^*_i$ (which happens with probability 1/2). By the definition of RF_i and by $\mathsf{m}^*_i = b$ we have $\mathsf{RF}_i(\mathsf{m}^*_{|i}) = \mathsf{RF}_{i-1}(\mathsf{m}^*_{|i-1})$, which implies CHAL($\mathsf{m}^*$) is identically distributed in $\mathsf{G}_{1,i}$ and $\mathsf{G}_{1,i-1}$.

We now analyze the output distribution of the EVAL queries. First note that $\mathbf{t}$ is uniformly random over $\mathbb{Z}_q^k$ in both games $\mathsf{G}_{1,i}$ and $\mathsf{G}_{1,i-1}$. As for the distribution of u, we only need to consider the case $\mathsf{m}_i = 1-b$, since u_m for $\mathsf{m}_i = b$ is identically distributed in games $\mathsf{G}_{1,i}$ and $\mathsf{G}_{1,i-1}$. Assume $\mathsf{m}_i = 1-b$. Write $\mathbf{H}_c = \mathbf{A}\mathbf{W}_c + \mathbf{R}_c$ for some $\mathbf{W}_c \in \mathbb{Z}_q^k$, where $\mathbf{R}_c = 0$ (i.e., $\mathbf{H}$ is from the $\mathcal{D}_k$-MDDH distribution) or $\mathbf{R}_c$ is uniform. Then,

$$\begin{aligned} u_\mathsf{m} &= \sum_{j \neq i} \mathbf{x}_{j,\mathsf{m}_j}^\top \mathbf{t}_\mathsf{m} + \mathbf{r}^\top \mathbf{A}(\mathbf{s}'_\mathsf{m} + \mathbf{W}_c) + \mathbf{r}^\top \mathbf{R}_c + \mathsf{RF}_{i-1}(\mathsf{m}_{|i-1}) \\ &= \sum_{j \neq i} \mathbf{x}_{j,\mathsf{m}_j}^\top \mathbf{t}_\mathsf{m} + \mathbf{x}_{i,1-b}^\top \underbrace{\overline{\mathbf{A}}(\mathbf{s}'_\mathsf{m} + \mathbf{W}_c)}_{\mathbf{t}_\mathsf{m}} + \mathbf{r}^\top \mathbf{R}_c + \mathsf{RF}_{i-1}(\mathsf{m}_{|i-1}) \\ &= \sum_{j=0}^{|\mathsf{m}|} \mathbf{x}_{j,\mathsf{m}_j}^\top \mathbf{t}_\mathsf{m} + \mathbf{r}^\top \mathbf{R}_c + \mathsf{RF}_{i-1}(\mathsf{m}_{|i-1}). \end{aligned}$$

If $\mathbf{R}_c = 0$, then u_m is distributed as in game $\mathsf{G}_{1,i-1}$. If $\mathbf{R}_c$ is uniform, then define $\mathsf{RF}'(\mathsf{m}_{|i-1}) := \mathbf{r}^\top \mathbf{R}_c$ and u is distributed as in $\mathsf{G}_{1,i}$. ▮

Lemma 3.7 $\Pr[\mathsf{G}_{1,m}^\mathcal{A} \Rightarrow 1] = \Pr[\mathsf{G}_2^\mathcal{A} \Rightarrow 1]$

Proof: In $\mathsf{G}_{1,m}$, the values u_m computed in EVAL(m) are masked by $\mathsf{RF}_m(\mathsf{m})$ and are hence uniformly random for distinct m. ▮

Finally, we do all the previous steps in reverse order, as shown in Figure 4, where the index i of hybrid $\mathsf{H}_{1,i}$ starts with m and ends with 0. Clearly, $\mathsf{H}_2 = \mathsf{G}_2$ and $\mathsf{H}_0 = \mathsf{PR\text{-}CMA}_{\mathsf{rand}}$. Following the arguments of Lemmas 3.5 to 3.7 in reverse order, one obtains the following lemma.

Lemma 3.8 *There exists an adversary $\mathcal{B}_1$ with $\mathbf{T}(\mathcal{B}_1) \approx \mathbf{T}(\mathcal{A})$ and $2m(\mathbf{Adv}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}_1) - 1/(q-1)) \geq$ $|\Pr[\mathsf{G}_2^\mathcal{A} \Rightarrow 1] - \Pr[\mathsf{PR\text{-}CMA}_{\mathsf{rand}}^\mathcal{A} \Rightarrow 1]|$.*

Initialize: // Games H_0, $\mathsf{H}_{1,i}$, $\boxed{\mathsf{H}_2}$
$\mathbf{B} \xleftarrow{\$} \mathbb{Z}_q^{k\times k}$; $\boxed{x'_0 \leftarrow_\$ \mathbb{Z}_q}$
For $i = 1, \dots, m : \mathbf{x}_{i,0}, \mathbf{x}_{i,1} \leftarrow \mathbb{Z}_q^k$
Return ε
 	
Chal(m^*): //Games H_0- H_2, one query
$h \xleftarrow{\$} \mathbb{Z}_q$ $\mathbf{h}_0 \xleftarrow{\$} \mathbb{Z}_q^k$; $h_1 \xleftarrow{\$} \mathbb{Z}_q$
Return $([h]_1, [\mathbf{h}_0]_1, [h_1]_T)$
	Eval(m): // Games H_0, $\boxed{\mathsf{H}_{1,i}}$, H_2
	$\mathcal{Q}_\mathcal{M} = \mathcal{Q}_\mathcal{M} \cup \{\mathsf{m}\}$
	$\mathbf{s}_\mathsf{m} \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{t}_\mathsf{m} = \mathbf{B}\mathbf{s}_\mathsf{m}$
	$u_\mathsf{m} \xleftarrow{\$} \mathbb{Z}_q$
	$\boxed{u_\mathsf{m} = (\sum_{j=1}^m \mathbf{x}_{j,\mathsf{m}_j}^\top)\mathbf{t}_\mathsf{m} + \mathsf{RF}_i(\mathsf{m}_{\mid i})}$
	$u_\mathsf{m} = (\sum_{j=1}^m \mathbf{x}_{j,\mathsf{m}_j}^\top)\mathbf{t}_\mathsf{m} + x'_0$
	Return $([\mathbf{t}_\mathsf{m}]_2, [u_\mathsf{m}]_2)$
	
	Finalize($d \in \{0,1\}$): // Games H_0-H_2
	Return $d \wedge (\mathsf{m}^* \notin \mathcal{Q}_\mathcal{M})$

Figure 4: Games H_0, $\mathsf{H}_{1,i}$ $(m \geq i \geq 0)$ and H_2 for the proof of Lemma 3.8.

This completes the proof of Theorem 3.3. ▮

3.3 An Affine MAC from Hash Proof System

Let $\mathcal{D}_k$ be a matrix distribution. We now combine the hash proof system for the subset membership problem induced by the $\mathcal{D}_k$-MDDH assumption from [13] with the generic MAC construction from [12] and obtain the following $\mathsf{MAC}_\mathsf{HPS}[\mathcal{D}_k]$ for $\mathcal{M} = \mathbb{Z}_q^\ell$.

$\mathsf{Gen}_\mathsf{MAC}(\mathsf{par})$:	$\mathsf{Tag}(\mathsf{sk}_\mathsf{MAC}, \mathsf{m})$:	$\mathsf{Ver}(\mathsf{sk}_\mathsf{MAC}, \tau, \mathsf{m})$:
$\mathbf{B} \xleftarrow{\$} \mathcal{D}_k$ $\mathbf{x}_0, \dots, \mathbf{x}_\ell \xleftarrow{\$} \mathbb{Z}_q^{k+1}$ $x'_0 \xleftarrow{\$} \mathbb{Z}_q$ Return $\mathsf{sk}_\mathsf{MAC} = (\mathbf{B}, \mathbf{x}_0, \dots, \mathbf{x}_\ell, x'_0)$	$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k$ $\mathbf{t} = \mathbf{B}\mathbf{s} \in \mathbb{Z}_q^{k+1}$ $u = (\mathbf{x}_0^\top + \sum_{i=1}^{\lvert\mathsf{m}\rvert} \mathsf{m}_i \cdot \mathbf{x}_i^\top)\mathbf{t} + x'_0 \in \mathbb{Z}_q$ Return $\tau = ([\mathbf{t}]_2, [u]_2) \in \mathbb{G}_2^{k+1} \times \mathbb{G}_2$	If $u = (\mathbf{x}_0^\top + \sum_{i=1}^{\lvert\mathsf{m}\rvert} \mathsf{m}_i \cdot \mathbf{x}_i^\top)\mathbf{t} + x'_0$ then return 1 Else return 0

Note that $\mathsf{MAC}_\mathsf{HPS}[\mathcal{D}_k]$ is n-affine over $\mathbb{Z}_q^n$ with $n = k+1$, $n' = k$, $\ell' = 0$, and defining functions $f_0(\mathsf{m}) = 1$, $f_i(\mathsf{m}) = \mathsf{m}_i$, and $f'_0(\mathsf{m}) = 1$, where m_i is the i-th component of m. For the moment we use $\ell = 1$ which already gives a MAC with exponential message space $\mathcal{M} = \mathbb{Z}_q$.

Combining [13, 12] we obtain that $\mathsf{MAC}_\mathsf{HPS}[\mathcal{D}_k]$ is UF-CMA under the $\mathcal{D}_k$-MDDH assumption. The proof extends to show even PR-CMA security. Compared to $\mathsf{MAC}_\mathsf{NR}[\mathcal{D}_k]$, we lose the tight reduction, but gain much shorter public parameters.

Theorem 3.9 $\mathsf{MAC}_\mathsf{HPS}[\mathcal{D}_k]$ *is* PR-CMA*-secure under the* $\mathcal{D}_k$-MDDH *assumption. In particular, for all adversaries* $\mathcal{A}$ *there exists an adversary* $\mathcal{D}$ *with* $\mathbf{T}(\mathcal{A}) \approx \mathbf{T}(\mathcal{D})$ *and* $\mathsf{Adv}^{\mathsf{pr\text{-}cma}}_{\mathsf{MAC}_\mathsf{HPS}[\mathcal{D}_k]}(\mathcal{A}) \leq 2Q(\mathbf{Adv}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{D}) + 1/q)$*, where* Q *is the maximal number of queries to* Eval$(\cdot)$*.*

Proof: We prove Theorem 3.9 by defining a sequence of intermediate games as in Figure 5. Let $\mathcal{A}$ be an adversary against the PR-CMA-security of $\mathsf{MAC}_\mathsf{HPS}[\mathcal{D}_k]$. Game G_0 is the real attack game. In games $\mathsf{G}_{1,i}$, the first $i-1$ queries to the Eval oracle are answered with uniform values in $\mathbb{G}_2^{k+1} \times \mathbb{G}_2$ and the rest are answered as in the real scheme. To interpolate between $\mathsf{G}_{1,i}$ and $\mathsf{G}_{1,i+1}$, we also define $\mathsf{G}'_{1,i}$, which answers the i-th query to Eval by picking a random $\mathbf{t} \xleftarrow{\$} \mathbb{Z}_q^{k+1}$. By definition, we have $\mathsf{G}_0 = \mathsf{G}_{1,1}$.

Lemma 3.10 $\Pr[\mathsf{PR}\text{-}\mathsf{CMA}^\mathcal{A}_\mathsf{real} \Rightarrow 1] = \Pr[\mathsf{G}_0^\mathcal{A} \Rightarrow 1] = \Pr[\mathsf{G}_{1,1}^\mathcal{A} \Rightarrow 1]$.

Lemma 3.11 *There exists an adversary* $\mathcal{B}$ *with* $\mathbf{T}(\mathcal{B}) \approx \mathbf{T}(\mathcal{A})$ *and* $\mathbf{Adv}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}) \geq |\Pr[\mathsf{G}'^\mathcal{A}_{1,i} \Rightarrow 1] - \Pr[\mathsf{G}^\mathcal{A}_{1,i} \Rightarrow 1]|$.

Proof: Games $\mathsf{G}_{1,i}$ and $\mathsf{G}'_{1,i}$ only differ in the distribution of $\mathbf{t}$ returned by the Eval oracle for its i-th query, namely, $\mathbf{t} \in \mathit{span}(\mathbf{B})$ or uniform. From that, we obtain a straightforward reduction to the $\mathcal{D}_k$-MDDH Assumption. ▮

$\underline{\text{INITIALIZE:}}$ // Games G_0-G_2

$\mathbf{B} \xleftarrow{\$} \mathcal{D}_k$; $x_0' \xleftarrow{\$} \mathbb{Z}_q$

For $j = 0, \dots, \ell : \mathbf{x}_j \xleftarrow{\$} \mathbb{Z}_q^{k+1}$

Return ε

$\underline{\text{CHAL}(\mathsf{m}^*)\text{:}}$ //Games G_0-$\mathsf{G}_{1,Q+1}$, $\boxed{\mathsf{G}_2}$

$h \xleftarrow{\$} \mathbb{Z}_q$

$\mathbf{h}_0 = (\mathbf{x_0} + \sum \mathsf{m}_j^* \cdot \mathbf{x}_j)h \in \mathbb{Z}_q^{k+1}$; $h_1 = x_0' h \in \mathbb{Z}_q$

$\boxed{\mathbf{h}_0 \xleftarrow{\$} \mathbb{Z}_q^{k+1}; \ h_1 \xleftarrow{\$} \mathbb{Z}_q}$

Return $([h]_1, [\mathbf{h}_0]_1, [h_1]_T)$

$\underline{\text{FINALIZE}(d \in \{0,1\})\text{:}}$ // Games G_0-G_2

Return $d \wedge (\mathsf{m}^* \notin \mathcal{Q}_{\mathcal{M}})$

$\underline{\text{EVAL}(\mathsf{m})\text{:}}$ //Game G_2

$\mathcal{Q}_{\mathcal{M}} = \mathcal{Q}_{\mathcal{M}} \cup \{\mathsf{m}\}$

$(\mathbf{t}, u) \xleftarrow{\$} \mathbb{Z}_q^{k+1} \times \mathbb{Z}_q$

Return $([\mathbf{t}]_2, [u]_2)$

$\underline{\text{EVAL}(\mathsf{m})\text{:}}$ // Game G_0

$\mathcal{Q}_{\mathcal{M}} = \mathcal{Q}_{\mathcal{M}} \cup \{\mathsf{m}\}$

$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k, \mathbf{t} = \mathbf{Bs} \in \mathbb{Z}_q^{k+1}$

$u = (\mathbf{x}_0^\top + \sum_{j=1}^{m} \mathsf{m}_j \cdot \mathbf{x}_j^\top)\mathbf{t} + x_0'$

Return $([\mathbf{t}]_2, [u]_2)$

$\underline{\text{EVAL}(\mathsf{m})\text{:}}$ // Games $\mathsf{G}_{1,i}$,$\boxed{\mathsf{G}_{1,i}'}$

$\mathcal{Q}_{\mathcal{M}} = \mathcal{Q}_{\mathcal{M}} \cup \{\mathsf{m}\}$ // Let m be the c-th query $(1 \le c \le Q)$

If $c < i$ then

  $(\mathbf{t}, u) \xleftarrow{\$} \mathbb{Z}_q^{k+1} \times \mathbb{Z}_q$

If $c > i$ then

  $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k, \mathbf{t} = \mathbf{Bs}$; $u = (\mathbf{x}_0^\top + \sum_{j=1}^{|\mathsf{m}|} \mathsf{m}_j \cdot \mathbf{x}_j^\top)\mathbf{t} + x_0'$

If $c = i$ then

  $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k, \mathbf{t} = \mathbf{Bs}$

  $\boxed{\mathbf{t} \xleftarrow{\$} \mathbb{Z}_q^{k+1}}$

  $u = (\mathbf{x}_0^\top + \sum_{j=1}^{|\mathsf{m}|} \mathsf{m}_j \cdot \mathbf{x}_j^\top)\mathbf{t} + x_0'$

Return $([\mathbf{t}]_2, [u]_2)$

Figure 5: Games $\mathsf{G}_0, (\mathsf{G}_{1,i}, \mathsf{G}_{1,i}')_{1 \le i \le Q}, \mathsf{G}_{1,Q+1}, \mathsf{G}_2$ for the proof of Theorem 3.9.

Lemma 3.12 $|\Pr[\mathsf{G}_{1,i+1}^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathsf{G}_{1,i}'^{\mathcal{A}} \Rightarrow 1]| \le 1/q$.

Proof: At a high level, these two games are only separated by the 2-universality of the underlying hash proof system. Let m be the i-th query to EVAL and let $([\mathbf{t}]_2, [u]_2)$ be its tag. As $\mathsf{m} \neq \mathsf{m}^*$, there exists an index i' such that $\mathsf{m}_{i'} \neq \mathsf{m}_{i'}^*$, where $\mathsf{m}_{i'}$ (resp. $\mathsf{m}_{i'}^*$) denotes the i'-th entry of m (resp. m^*). We use an information-theoretic argument to show that in $\mathsf{G}_{1,i}'$ the value $u - x_0'$ is uniformly random. For simplicity, we assume x_0' and $\mathbf{x}_j$ ($j \notin \{0, i'\}$) are known to $\mathcal{A}$. Information-theoretically, adversary $\mathcal{A}$ may also learn $\mathbf{B}^\top \mathbf{x}_0$ and $\mathbf{B}^\top \mathbf{x}_{i'}$ from the c-th query with $c > i$. Thus, $\mathcal{A}$ information-theoretically obtains the following equations in the unknown variables $\begin{pmatrix} \mathbf{x}_0 \\ \mathbf{x}_{i'} \end{pmatrix} \in \mathbb{Z}_q^{2(k+1)}$:

$$\begin{pmatrix} \mathbf{B}^\top \mathbf{x}_0 \\ \mathbf{B}^\top \mathbf{x}_{i'} \\ \mathbf{h}_0 \\ u - x_0' \end{pmatrix} = \underbrace{\begin{pmatrix} \mathbf{B}^\top & \mathbf{0} \\ \mathbf{0} & \mathbf{B}^\top \\ h \cdot \mathbf{I}_{k+1} & \mathsf{m}_{i'}^* h \cdot \mathbf{I}_{k+1} \\ \mathbf{t}^\top & \mathsf{m}_{i'} \mathbf{t}^\top \end{pmatrix}}_{=:\mathbf{M} \in \mathbb{Z}_q^{(3k+2) \times (2k+2)}} \cdot \begin{pmatrix} \mathbf{x}_0 \\ \mathbf{x}_{i'} \end{pmatrix}$$

where $\mathbf{I}_{k+1}$ is the $(k+1) \times (k+1)$ identity matrix. To show that $u - x_0'$ is linearly independent of $\mathbf{B}^\top \mathbf{x}_0$, $\mathbf{B}^\top \mathbf{x}_{i'}$ and $\mathbf{h}_0$, we argue that the last row of $\mathbf{M}$ is linearly independent of all the other rows. Since $\mathbf{t} \notin \mathit{span}(\mathbf{B})$ (except with probability $1/q$), $\mathbf{t}^\top$ is independent of $\mathbf{B}^\top$; by $\mathsf{m}_{i'} \neq \mathsf{m}_{i'}^*$, the last row of $\mathbf{M}$ is linearly independent of rows $2k+1$ to $3k+1$. We conclude that u is uniformly random in $\mathcal{A}$'s view. ▌

Lemma 3.13 $\Pr[\mathsf{G}_2^{\mathcal{A}} \Rightarrow 1] = \Pr[\mathsf{G}_{1,Q+1}^{\mathcal{A}} \Rightarrow 1]$.

Proof: Note that $\mathcal{A}$ can ask at most Q-many EVAL queries. In both $\mathsf{G}_{1,Q+1}$ and G_2, all answers of EVAL are uniformly at random and independent of the secret keys $(x_0', \mathbf{x}_0, \dots, \mathbf{x}_\ell)$. Hence, the values $\mathbf{h}_0$ and h_1 from $\mathsf{G}_{1,Q+1}$ are uniform in the view of $\mathcal{A}$. ▌

We now do all the previous steps in the reverse order as in Figure 6. Then, by using the above arguments in a reverse order, we have the following lemma.

$\underline{\textsc{Initialize:}}$ // Games H_0-H_2
$\mathbf{B} \xleftarrow{\$} \mathcal{D}_k;\ x'_0 \leftarrow_\$ \mathbb{Z}_q$
For $j = 0, \ldots, \ell : \mathbf{x}_j \leftarrow_\$ \mathbb{Z}_q^{k+1}$
Return ε

$\underline{\textsc{Chal}(\mathsf{m}^*):}$ //Games H_0-H_2
$h \xleftarrow{\$} \mathbb{Z}_q;\ \mathbf{h}_0 \xleftarrow{\$} \mathbb{Z}_q^{k+1};\ h_1 \xleftarrow{\$} \mathbb{Z}_q$
Return $([h]_1, [\mathbf{h}_0]_1, [h_1]_T)$

$\underline{\textsc{Finalize}(d \in \{0,1\}):}$ // Games H_0-H_2
Return $d \wedge (\mathsf{m}^* \notin \mathcal{Q}_\mathcal{M})$

$\underline{\textsc{Eval}(\mathsf{m}):}$ //Game H_0
$\mathcal{Q}_\mathcal{M} = \mathcal{Q}_\mathcal{M} \cup \{\mathsf{m}\}$
$(\mathbf{t}, u) \xleftarrow{\$} \mathbb{Z}_q^{k+1} \times \mathbb{Z}_q$
Return $([\mathbf{t}]_2, [u]_2)$

$\underline{\textsc{Eval}(\mathsf{m}):}$ // Games $\mathsf{H}_{1,i}$, $\boxed{\mathsf{H}'_{1,i}}$
$\mathcal{Q}_\mathcal{M} = \mathcal{Q}_\mathcal{M} \cup \{\mathsf{m}\}$ // Let m be the c-th query $(1 \le c \le Q)$
If $c > i$ then
  $(\mathbf{t}, u) \xleftarrow{\$} \mathbb{Z}_q^{k+1} \times \mathbb{Z}_q$
If $c < i$ then
  $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k, \mathbf{t} = \mathbf{B}\mathbf{s};\ u = (\mathbf{x}_0^\top + \sum_{j=1}^{|\mathsf{m}|} \mathsf{m}_j \cdot \mathbf{x}_j^\top)\mathbf{t} + x'_0$
If $c = i$ then
  $\mathbf{t} \xleftarrow{\$} \mathbb{Z}_q^{k+1}$
  $\boxed{\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k;\ \mathbf{t} = \mathbf{B}\mathbf{s} \in \mathbb{Z}_q^{k+1}}$
  $u = (\mathbf{x}_0^\top + \sum_{j=1}^{|\mathsf{m}|} \mathsf{m}_j \cdot \mathbf{x}_j^\top)\mathbf{t} + x'_0$
Return $([\mathbf{t}]_2, [u]_2)$

$\underline{\textsc{Eval}(\mathsf{m}):}$ // Game H_2
$\mathcal{Q}_\mathcal{M} = \mathcal{Q}_\mathcal{M} \cup \{\mathsf{m}\}$
$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k, \mathbf{t} = \mathbf{B}\mathbf{s}$
$u = (\mathbf{x}_0^\top + \sum_{i=1}^{|\mathsf{m}|} \mathsf{m}_i \cdot \mathbf{x}_i^\top)\mathbf{t} + x'_0$
Return $([\mathbf{t}]_2, [u]_2)$

Figure 6: Games $\mathsf{H}_0, (\mathsf{H}_{1,i}, \mathsf{H}'_{1,i})_{1 \le i \le Q}, \mathsf{H}_{1,Q+1}, \mathsf{H}_2$ for the proof of Lemma 3.14.

Lemma 3.14 *There exists an adversary $\mathcal{B}$ with $\mathbf{T}(\mathcal{B}) \approx \mathbf{T}(\mathcal{A})$ and $Q(\mathbf{Adv}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}) + 1/q) \ge |\Pr[\mathsf{PR\text{-}CMA}^\mathcal{A}_{\mathsf{rand}} \Rightarrow 1] - \Pr[\mathsf{G}_2^\mathcal{A} \Rightarrow 1]|$.*

Theorem 3.9 follows by combining Lemmas 3.10-3.14. ▌

4 Identity-based Encryption from Affine MACs

In this section, we will present our transformation $\mathsf{IBE}[\mathsf{MAC}, \mathcal{D}_k]$ from affine MACs to IBE based on the $\mathcal{D}_k$-MDDH assumption.

4.1 Identity-based Key Encapsulation

We now recall syntax and security of IBE in terms of an ID-based key encapsulation mechanism IBKEM. Every IBKEM can be transformed into an ID-based encryption scheme IBE using a (one-time secure) symmetric cipher.

Definition 4.1 (Identity-based Key Encapsulation Scheme) *An identity-based key encapsulation (IBKEM) scheme* IBKEM *consists of four PPT algorithms* $\mathsf{IBKEM} = (\mathsf{Gen}, \mathsf{USKGen}, \mathsf{Enc}, \mathsf{Dec})$ *with the following properties.*

- *The probabilistic key generation algorithm* $\mathsf{Gen}(1^\lambda)$ *returns the (master) public/secret key* $(\mathsf{pk}, \mathsf{sk})$. *We assume that* pk *implicitly defines an identity space* $\mathcal{ID}$, *a key space* $\mathcal{K}$, *and ciphertext space* $\mathcal{C}$.
- *The probabilistic user secret key generation algorithm* $\mathsf{USKGen}(\mathsf{sk}, \mathsf{id})$ *returns the user secret-key* $\mathsf{usk}[\mathsf{id}]$ *for identity* $\mathsf{id} \in \mathcal{ID}$.
- *The probabilistic encapsulation algorithm* $\mathsf{Enc}(\mathsf{pk}, \mathsf{id})$ *returns the symmetric key* $\mathsf{K} \in \mathcal{K}$ *together with a ciphertext* $\mathsf{C} \in \mathcal{C}$ *with respect to identity* id.
- *The deterministic decapsulation algorithm* $\mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id}, \mathsf{C})$ *returns the decapsulated key* $\mathsf{K} \in \mathcal{K}$ *or the reject symbol* $\perp$.

For perfect correctness we require that for all $\lambda \in \mathbb{N}$, *all pairs* $(\mathsf{pk}, \mathsf{sk})$ *generated by* $\mathsf{Gen}(1^\lambda)$, *all identities* $\mathsf{id} \in \mathcal{ID}$, *all* $\mathsf{usk}[\mathsf{id}]$ *generated by* $\mathsf{USKGen}(\mathsf{sk}, \mathsf{id})$ *and all* (K, C) *output by* $\mathsf{Enc}(\mathsf{pk}, \mathsf{id})$*:*

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

<u>**Procedure** INITIALIZE:</u> $(\mathsf{pk},\mathsf{sk}) \xleftarrow{\$} \mathsf{Gen}(1^\lambda)$ Return pk <u>**Procedure** USKGEN(id):</u> $\mathcal{Q}_{\mathcal{ID}} \leftarrow \mathcal{Q}_{\mathcal{ID}} \cup \{\mathsf{id}\}$ Return $\mathsf{usk}[\mathsf{id}] \xleftarrow{\$} \mathsf{USKGen}(\mathsf{sk},\mathsf{id})$	<u>**Procedure** ENC(id*):</u> //one query $(\mathsf{K}^*,\mathsf{C}^*) \xleftarrow{\$} \mathsf{Enc}(\mathsf{pk},\mathsf{id}^*)$ $\boxed{\mathsf{K}^* \xleftarrow{\$} \mathcal{K}; \mathsf{C}^* \xleftarrow{\$} \mathcal{C}}$ Return $(\mathsf{K}^*,\mathsf{C}^*)$ <u>**Procedure** FINALIZE(β):</u> Return $(\mathsf{id}^* \notin \mathcal{Q}_{\mathcal{ID}}) \wedge \beta$

Figure 7: Security Games $\mathsf{PR\text{-}ID\text{-}CPA}_{\mathsf{real}}$ and $\boxed{\mathsf{PR\text{-}ID\text{-}CPA}_{\mathsf{rand}}}$ for defining PR-ID-CPA-security.

The security requirements for an IBKEM we consider here are indistinguishability and anonymity against chosen plaintext and identity attacks (IND-ID-CPA and ANON-ID-CPA). Instead of defining both security notions separately, we define pseudorandom ciphertexts against chosen plaintext and identity attacks (PR-ID-CPA) which means that challenge key and ciphertext are both pseudorandom. Note that PR-ID-CPA trivially implies IND-ID-CPA and ANON-ID-CPA.

We define PR-ID-CPA-security of IBKEM formally via the games given in Figure 7.

Definition 4.2 (PR-ID-CPA **Security**) *An identity-based key encapsulation scheme* IBKEM *is* PR-ID-CPA-*secure if for all PPT $\mathcal{A}$,* $\mathsf{Adv}^{\mathsf{pr\text{-}id\text{-}cpa}}_{\mathsf{IBKEM}}(\mathcal{A}) := |\Pr[\mathsf{PR\text{-}ID\text{-}CPA}^{\mathcal{A}}_{\mathsf{real}} \Rightarrow 1] - \Pr[\mathsf{PR\text{-}ID\text{-}CPA}^{\mathcal{A}}_{\mathsf{rand}} \Rightarrow 1]|$ *is negligible.*

4.2 The Transformation

Let $\mathcal{D}_k$ be a matrix distribution that outputs matrices $\mathbf{A} \in \mathbb{Z}_q^{(k+1)\times k}$. Let MAC be an affine MAC over $\mathbb{Z}_q^n$ with message space $\mathcal{ID}$. Our IBKEM $\mathsf{IBKEM}[\mathsf{MAC},\mathcal{D}_k] = (\mathsf{Gen},\mathsf{USKGen},\mathsf{Enc},\mathsf{Dec})$ for key-space $\mathcal{K} = \mathbb{G}_T$ and identity space $\mathcal{ID}$ is defined as follows.

<u>$\mathsf{Gen}(\mathsf{par})$:</u> $\mathbf{A} \xleftarrow{\$} \mathcal{D}_k$ $\mathsf{sk}_{\mathsf{MAC}} = (\mathbf{B}, \mathbf{x}_0, \ldots, \mathbf{x}_\ell, x'_0, \ldots, x'_{\ell'}) \xleftarrow{\$} \mathsf{Gen}_{\mathsf{MAC}}(\mathsf{par})$ For $i = 0, \ldots, \ell : \mathbf{Y}_i \xleftarrow{\$} \mathbb{Z}_q^{k\times n}; \mathbf{Z}_i = (\mathbf{Y}_i^\top \mid \mathbf{x}_i) \cdot \mathbf{A} \in \mathbb{Z}_q^{n\times k}$ For $i = 0, \ldots, \ell' : \mathbf{y}'_i \xleftarrow{\$} \mathbb{Z}_q^{k}; \mathbf{z}'_i = (\mathbf{y}'^\top_i \mid x'_i) \cdot \mathbf{A} \in \mathbb{Z}_q^{1\times k}$ $\mathsf{pk} := (\mathcal{G}, [\mathbf{A}]_1, ([\mathbf{Z}_i]_1)_{0\le i\le \ell}, ([\mathbf{z}'_i]_1)_{0\le i\le \ell'})$ $\mathsf{sk} := (\mathsf{sk}_{\mathsf{MAC}}, (\mathbf{Y}_i)_{0\le i\le \ell}, (\mathbf{y}'_i)_{0\le i\le \ell'})$ Return $(\mathsf{pk},\mathsf{sk})$ <u>$\mathsf{USKGen}(\mathsf{sk},\mathsf{id})$:</u> $([\mathbf{t}]_2, [u]_2) \xleftarrow{\$} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{id})$ $\mathbf{v} = \sum_{i=0}^{\ell} f_i(\mathsf{id})\mathbf{Y}_i\mathbf{t} + \sum_{i=0}^{\ell'} f'_i(\mathsf{id})\mathbf{y}'_i \in \mathbb{Z}_q^k$ Return $\mathsf{usk}[\mathsf{id}] := ([\mathbf{t}]_2, [u]_2, [\mathbf{v}]_2) \in \mathbb{G}_2^{n+1+k}$	<u>$\mathsf{Enc}(\mathsf{pk},\mathsf{id})$:</u> $\mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^k$ $\mathbf{c}_0 = \mathbf{A}\mathbf{r} \in \mathbb{Z}_q^{k+1}$ $\mathbf{c}_1 = (\sum_{i=0}^{\ell} f_i(\mathsf{id})\mathbf{Z}_i) \cdot \mathbf{r} \in \mathbb{Z}_q^n$ $K = (\sum_{i=0}^{\ell'} f'_i(\mathsf{id})\mathbf{z}'_i) \cdot \mathbf{r} \in \mathbb{Z}_q$. Return $\mathsf{K} = [K]_T$ and $\mathsf{C} = ([\mathbf{c}_0]_1, [\mathbf{c}_1]_1) \in \mathbb{G}_1^{n+k+1}$ <u>$\mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id}, \mathsf{C})$:</u> Parse $\mathsf{usk}[\mathsf{id}] = ([\mathbf{t}]_2, [u]_2, [\mathbf{v}]_2)$ Parse $\mathsf{C} = ([\mathbf{c}_0]_1, [\mathbf{c}_1]_1)$ $\mathsf{K} = e([\mathbf{c}_0]_1, \begin{bmatrix}\mathbf{v}\\ u\end{bmatrix}_2) - e([\mathbf{c}_1]_1, [\mathbf{t}]_2)$ Return $\mathsf{K} \in \mathbb{G}_T$

The intuition behind our construction is that the values $[\mathbf{Z}_i]_1, [\mathbf{z}'_i]_1$ from pk can be viewed as perfectly hiding commitments to the secrets keys $\mathsf{sk}_{\mathsf{MAC}} = (\mathbf{x}_1, \ldots, \mathbf{x}_\ell, x'_1, \ldots, x'_{\ell'})$ of MAC. User secret key generation computes the MAC tag $\tau = ([\mathbf{t}]_2, [u]_2) \xleftarrow{\$} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}})$ plus a "non-interactive zero-knowledge proof" $[\mathbf{v}]_2$ proving that τ was computed correctly with respect to the commitments. As the MAC is affine, the NIZK proof has a very simple structure. The encryption algorithm is derived from a randomized version of the NIZK verification equation. Here we again make use of the affine structure of MAC.

To show correctness of $\mathsf{IBKEM}[\mathsf{MAC},\mathcal{D}_k]$, let (K,C) be the output of $\mathsf{Enc}(\mathsf{pk},\mathsf{id})$ and let $\mathsf{usk}[\mathsf{id}]$ be the

$\underline{\textsc{Initialize:}}$ // Games G_0-G_4

$\mathcal{G} \xleftarrow{\$} \mathsf{GGen}(1^\lambda); \mathbf{A} \xleftarrow{\$} \mathcal{D}_k$
$\mathsf{sk}_{\mathsf{MAC}} = (\mathbf{B}, \mathbf{x}_0, \ldots, \mathbf{x}_\ell, x'_0, \ldots, x'_{\ell'}) \xleftarrow{\$} \mathsf{Gen}_{\mathsf{MAC}}(\mathcal{G})$
For $i = 0, \ldots, \ell : \mathbf{Y}_i \xleftarrow{\$} \mathbb{Z}_q^{k \times n}; \mathbf{Z}_i = (\mathbf{Y}_i^\top \mid \mathbf{x}_i) \cdot \mathbf{A} \in \mathbb{Z}_q^{n \times k}$
For $i = 0, \ldots, \ell' : \mathbf{y}'_i \xleftarrow{\$} \mathbb{Z}_q^k; \mathbf{z}'_i = (\mathbf{y}_i'^\top \mid x'_i) \cdot \mathbf{A} \in \mathbb{Z}_q^{1 \times k}$
$\mathsf{pk} := (\mathcal{G}, [\mathbf{A}]_1, ([\mathbf{Z}_i]_1)_{0 \le i \le \ell}, ([\mathbf{z}'_i]_1)_{0 \le i \le \ell'})$
$\mathsf{sk} := (\mathsf{sk}_{\mathsf{MAC}}, (\mathbf{Y}_i)_{0 \le i \le \ell}, (\mathbf{y}'_i)_{0 \le i \le \ell'})$
Return pk

$\underline{\textsc{Finalize}(\beta):}$ //Games G_0-G_4

Return $(\mathsf{id}^* \notin \mathcal{Q}_{\mathcal{ID}}) \wedge \beta$

$\underline{\textsc{USKGen}(\mathsf{id}):}$ //Games G_0-G_2, G_3-G_4

$\mathcal{Q}_{\mathcal{ID}} = \mathcal{Q}_{\mathcal{ID}} \cup \{\mathsf{id}\}$
$([\mathbf{t}]_2, [u]_2) \xleftarrow{\$} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{id})$
$\mathbf{v} = \sum_{i=0}^{\ell} f_i(\mathsf{id}) \mathbf{Y}_i \mathbf{t} + \sum_{i=0}^{\ell'} f'_i(\mathsf{id}) \mathbf{y}'_i \in \mathbb{Z}_q^k$
$\mathbf{v}^\top = (\mathbf{t}^\top \sum f_i(\mathsf{id}) \mathbf{Z}_i + \sum f'_i(\mathsf{id}) \mathbf{z}'_i - u \cdot \underline{\mathbf{A}}) \cdot \overline{\mathbf{A}}^{-1}$
$\mathsf{usk}[\mathsf{id}] := ([\mathbf{t}]_2, [u]_2, [\mathbf{v}]_2) \in \mathbb{G}_2^n \times \mathbb{G}_2^1 \times \mathbb{G}_2^k$
Return $\mathsf{usk}[\mathsf{id}]$

$\underline{\textsc{Enc}(\mathsf{id}^*):}$ //Games G_0, $\boxed{\mathsf{G}_1\text{-}\mathsf{G}_2}$, $\boxed{\mathsf{G}_2}$ G_3

$\mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^k;$
$\mathbf{c}_0^* = \mathbf{A}\mathbf{r} \in \mathbb{Z}_q^{k+1}$
$\boxed{\mathbf{c}_0^* \xleftarrow{\$} \mathbb{Z}_q^{k+1}}$
$h \xleftarrow{\$} \mathbb{Z}_q; \overline{\mathbf{c}_0^*} \xleftarrow{\$} \mathbb{Z}_q^k; \underline{\mathbf{c}_0^*} := h + \underline{\mathbf{A}} \cdot \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}_0^*} \in \mathbb{Z}_q$
$\mathbf{c}_1^* = (\sum_{i=0}^{\ell} f_i(\mathsf{id}^*) \mathbf{Z}_i) \mathbf{r} \in \mathbb{Z}_q^n$
$\boxed{\mathbf{c}_1^* = \sum_{i=0}^{\ell} f_i(\mathsf{id}^*)(\mathbf{Y}_i^\top \mid \mathbf{x}_i) \mathbf{c}_0^* \in \mathbb{Z}_q^n}$
$\mathbf{c}_1^* = \sum_{i=0}^{\ell} f_i(\mathsf{id}^*)(\mathbf{Z}_i \cdot \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}_0^*} + \mathbf{x}_i \cdot h)$
$K^* = \sum_{i=0}^{\ell'} f'_i(\mathsf{id}^*) \mathbf{z}'_i \cdot \mathbf{r} \in \mathbb{Z}_q.$
$\boxed{K^* = \sum_{i=0}^{\ell'} f'_i(\mathsf{id}^*)(\mathbf{y}_i'^\top \mid x'_i) \mathbf{c}_0^* \in \mathbb{Z}_q}$
$K^* = \sum_{i=0}^{\ell'} f'_i(\mathsf{id}^*)(\mathbf{z}'_i \cdot \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}_0^*} + x'_i \cdot h)$
Return $\mathsf{K}^* = [K^*]_T$ and $\mathsf{C}^* = ([\mathbf{c}_0^*]_1, [\mathbf{c}_1^*]_1)$

$\underline{\textsc{Enc}(\mathsf{id}^*):}$ //Game G_4

$\mathsf{K}^* \xleftarrow{\$} \mathbb{G}_T$ and $\mathsf{C}^* \xleftarrow{\$} \mathbb{G}_1^{n+k+1}$
Return K^* and C^*

Figure 8: Games G_0-G_4 for the proof of Theorem 4.3.

---

output of $\mathsf{USKGen}(\mathsf{sk}, \mathsf{id})$. By Equation (3) in Section 3, we have

$$e([\mathbf{c}_0]_1, \begin{bmatrix} \mathbf{v} \\ u \end{bmatrix}_2) = \left[(\mathbf{A}\mathbf{r})^\top \cdot \begin{pmatrix} \sum_{i=0}^{\ell} f_i(\mathsf{id}) \mathbf{Y}_i \mathbf{t} + \sum_{i=0}^{\ell'} f'_i(\mathsf{id}) \mathbf{y}'_i \\ \sum_{i=0}^{\ell} f_i(\mathsf{id}) \mathbf{x}_i^\top \mathbf{t} + \sum_{i=0}^{\ell'} f'_i(\mathsf{id}) x'_i \end{pmatrix} \right]_T$$

$$e([\mathbf{c}_1]_1, [\mathbf{t}]_2) = \left[(\mathbf{A}\mathbf{r})^\top \begin{pmatrix} \sum f_i(\mathsf{id}) \mathbf{Y}_i \\ \sum f_i(\mathsf{id}) \mathbf{x}_i^\top \end{pmatrix} \cdot \mathbf{t} \right]_T$$

and the quotient of the two elements yields $\mathsf{K} = (\sum_{i=0}^{\ell'} f'_i(\mathsf{id}) \mathbf{z}'_i) \cdot \mathbf{r}$.

Theorem 4.3 *Under the* $\mathcal{D}_k$-MDDH *assumption relative to* GGen *in* $\mathbb{G}_1$ *and the* PR-CMA*-security of* MAC*,* $\mathsf{IBKEM}[\mathsf{MAC}, \mathcal{D}_k]$ *is a* PR-ID-CPA*-secure IBKEM. Particularly, for all adversaries* $\mathcal{A}$ *there exist adversaries* $\mathcal{B}_1$ *and* $\mathcal{B}_2$ *with* $\mathbf{T}(\mathcal{B}_1) \approx \mathbf{T}(\mathcal{A}) \approx \mathbf{T}(\mathcal{B}_2)$ *and* $\mathsf{Adv}^{\mathsf{pr\text{-}id\text{-}cpa}}_{\mathsf{IBKEM}[\mathsf{MAC}, \mathcal{D}_k]}(\mathcal{A}) \le \mathbf{Adv}_{\mathcal{D}_k, \mathsf{GGen}}(\mathcal{B}_1) + \mathsf{Adv}^{\mathsf{pr\text{-}cma}}_{\mathsf{MAC}}(\mathcal{B}_2)$.

Proof of Theorem 4.3: We prove Theorem 4.3 by defining a sequence of games G_0-G_4 as in Figure 8. Let $\mathcal{A}$ be an adversary against the PR-ID-CPA security of $\mathsf{IBKEM}_{\mathsf{MAC}, \mathcal{D}_k}$.

Lemma 4.4 $\Pr[\mathsf{PR}\text{-}\mathsf{ID}\text{-}\mathsf{CPA}^{\mathcal{A}}_{\mathsf{real}} \Rightarrow 1] = \Pr[\mathsf{G}_1^{\mathcal{A}} \Rightarrow 1] = \Pr[\mathsf{G}_0^{\mathcal{A}} \Rightarrow 1]$.

Proof: G_0 is the real attack game. In game G_1, we change the simulation of $\mathbf{c}_1^*$ and K^* in $\textsc{Enc}(\mathsf{id}^*)$ by substituting $\mathbf{Z}_i$ and $\mathbf{z}'_i$ with their respective definitions:

$$\mathbf{c}_1^* = \sum_{i=0}^{\ell} f_i(\mathsf{id}^*) \mathbf{Z}_i \mathbf{r} = \sum_{i=0}^{\ell} f_i(\mathsf{id}^*)(\mathbf{Y}_i^\top \mid \mathbf{x}_i) \mathbf{A}\mathbf{r} = \sum_{i=0}^{\ell} f_i(\mathsf{id}^*)(\mathbf{Y}_i^\top \mid \mathbf{x}_i) \mathbf{c}_0^*$$

and, similarly $K^* = \sum f'_i(\mathsf{id}^*)(\mathbf{y}_i'^\top \mid x'_i) \mathbf{A}\mathbf{r} = \sum f'_i(\mathsf{id}^*)(\mathbf{y}_i'^\top \mid x'_i) \mathbf{c}_0^*$. Thus, G_1 is identical to G_0. ▮

Lemma 4.5 *There exists an adversary* $\mathcal{B}_1$ *with* $\mathbf{T}(\mathcal{B}_1) \approx \mathbf{T}(\mathcal{A})$ *and* $\mathbf{Adv}_{\mathcal{D}_k, \mathsf{GGen}}(\mathcal{B}_1) \ge |\Pr[\mathsf{G}_2^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathsf{G}_1^{\mathcal{A}} \Rightarrow 1]|$.

Proof: The only difference between G_2 and G_1 is that $\mathbf{c}_0^*$ is chosen uniformly at random over $\mathbb{Z}_q^{k+1}$. It is easy to see that the joint distribution of $(\mathcal{G}, [\mathbf{A}]_1, [\mathbf{c}_0^*]_1)$ in G_1 is identical to the real $\mathcal{D}_k$-MDDH distribution and $(\mathcal{G}, [\mathbf{A}]_1, [\mathbf{c}_0^*]_1)$ in G_2 is identical to the random $\mathcal{D}_k$-MDDH distribution.

More formally, we build a distinguisher $\mathcal{B}_1$. $\mathcal{B}_1$ takes as input $(\mathcal{G}, [\mathbf{A}]_1, [\mathbf{b}]_1)$ and it has to distinguish if $\mathbf{b} = \mathbf{A}\mathbf{w}$ for some random vector $\mathbf{w} \in \mathbb{Z}_q^k$ or $\mathbf{b}$ is uniformly random. $\mathcal{B}_1$ simulates USKGen and Finalize the same way as in G_2 and G_1. We only describe the simulation of Initialize and Enc in Figure 9. Note that $\mathcal{B}_1$ knows the secrets $\mathbf{x}_i, x'_i, \mathbf{Y}_i, \mathbf{y}'_i$ explicitly over $\mathbb{Z}_q$. Hence, $\mathcal{B}_1$ can compute $([\mathbf{Z}_i]_1, ([\mathbf{z}'_i]_1)_{0\le i\le \ell})$ from pk and $([\mathbf{c}_1^*]_1, [K^*]_T)$ from from the encryption query from $[\mathbf{A}]_1$ and $[\mathbf{b}]_1$. If $\mathbf{b} = \mathbf{A}\mathbf{w}$ for $\mathbf{w} \xleftarrow{\$} \mathbb{Z}_q^k$,

Initialize:	Enc(id^*):
$\mathsf{sk}_{\mathsf{MAC}} = (\mathbf{B}, \mathbf{x}_0, \dots, \mathbf{x}_\ell, x'_0, \dots, x'_{\ell'}) \xleftarrow{\$} \mathsf{Gen}_{\mathsf{MAC}}(\mathcal{G})$	$\mathbf{c}_0^* := \mathbf{b} \in \mathbb{Z}_q^{k+1}$
For $i = 0, \dots, \ell$: $\mathbf{Y}_i \xleftarrow{\$} \mathbb{Z}_q^{k\times n}$; $\mathbf{Z}_i = (\mathbf{Y}_i^\top \mid \mathbf{x}_i) \cdot \mathbf{A}$	$\mathbf{c}_1^* = \sum_{i=0}^{\ell} f_i(\mathsf{id}^*)(\mathbf{Y}_i^\top \mid \mathbf{x}_i)\mathbf{c}_0^* \in \mathbb{Z}_q^n$
For $i = 0, \dots, \ell'$: $\mathbf{y}'_i \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{z}'_i = (\mathbf{y}_i'^\top \mid x'_i) \cdot \mathbf{A}$	$K^* = \sum_{i=0}^{\ell'} f'_i(\mathsf{id}^*)(\mathbf{y}_i'^\top \mid x'_i)\mathbf{c}_0^* \in \mathbb{Z}_q$
$\mathsf{pk} := (\mathcal{G}, [\mathbf{A}]_1, ([\mathbf{Z}_i]_1)_{0\le i\le\ell}, ([\mathbf{z}'_i]_1)_{0\le i\le\ell'})$	Return $\mathsf{K}^* = [K^*]_T$ and $\mathsf{C}^* = ([\mathbf{c}_0^*]_1, [\mathbf{c}_1^*]_1)$
$\mathsf{sk} := (\mathsf{sk}_{\mathsf{MAC}}, (\mathbf{Y}_i)_{0\le i\le\ell}, (\mathbf{y}'_i)_{0\le i\le\ell'})$	
Return pk	

Figure 9: Description of $\mathcal{B}_1(\mathcal{G}, [\mathbf{A}]_1, [\mathbf{b}]_1)$ for the proof of Lemma 4.5.

then the simulation is distributed as in G_1. If $\mathbf{b}$ is uniformly random, then the simulation is distributed as in G_2. ▌

Following the intuition of the construction, in Game G_3, we simulate the values $\mathbf{v}$ computed in the USKGen algorithm using a "perfect zero-knowledge" simulator, and Enc is simulated without using $(\mathbf{Y}_i)_{0\le i\le\ell}$ and $(\mathbf{y}'_i)_{0\le i\le\ell'}$, which is ready to conclude the proof by using the PR-CMA security of MAC.

Lemma 4.6 $\Pr[\mathsf{G}_3^{\mathcal{A}} \Rightarrow 1] = \Pr[\mathsf{G}_2^{\mathcal{A}} \Rightarrow 1]$.

Proof: G_3 does not use $(\mathbf{Y}_i)_{0\le i\le\ell}$ and $(\mathbf{y}'_i)_{0\le i\le\ell'}$ any more. We now show that the changes are purely conceptual. By $\mathbf{Z}_i = (\mathbf{Y}_i^\top \mid \mathbf{x}_i)\mathbf{A}$, we have $\mathbf{Y}_i^\top = (\mathbf{Z}_i - \mathbf{x}_i \cdot \underline{\mathbf{A}}) \cdot (\overline{\mathbf{A}})^{-1}$, and similarly we have $\mathbf{y}_i'^\top = (\mathbf{z}'_i - x'_i \cdot \underline{\mathbf{A}}) \cdot (\overline{\mathbf{A}})^{-1}$. For USKGen($\mathsf{id}$), by substituting $\mathbf{Y}_i^\top$ and $\mathbf{y}_i'^\top$, we obtain

$$\begin{aligned}
\mathbf{v}^\top &= \Big(\mathbf{t}^\top \sum f_i(\mathsf{id})(\mathbf{Z}_i - \mathbf{x}_i \cdot \underline{\mathbf{A}}) + \sum f'_i(\mathsf{id})(\mathbf{z}'_i - x'_i \cdot \underline{\mathbf{A}})\Big)\,(\overline{\mathbf{A}})^{-1} \\
&= \left(\mathbf{t}^\top \sum f_i(\mathsf{id})\mathbf{Z}_i + \sum f'_i(\mathsf{id})\mathbf{z}'_i - \underbrace{\Big(\mathbf{t}^\top \sum f_i(\mathsf{id})\mathbf{x}_i + \sum f'_i(\mathsf{id})x'_i\Big)}_{u} \cdot \underline{\mathbf{A}}\right)(\overline{\mathbf{A}})^{-1}.
\end{aligned}$$

Note that we can compute $[\mathbf{v}]_2$ in $\mathbb{G}_2$, since $\mathbf{A}$, $\mathbf{z}'_i$ and $\mathbf{Z}_i$ are known explicitly over $\mathbb{Z}_q$ and $[\mathbf{t}]_2$ and $[u]_2$ are known.

As for the distribution of Enc(id^*), it is easy to see that $\mathbf{c}_0^*$ is uniformly random, as in G_2. By $h = \underline{\mathbf{c}_0^*} - \underline{\mathbf{A}} \cdot \overline{\mathbf{A}}^{-1}\overline{\mathbf{c}_0^*}$, we have

$$\begin{aligned}
\mathbf{c}_1^* &= \sum f_i(\mathsf{id}_i^*)(\mathbf{Z}_i \cdot \overline{\mathbf{A}}^{-1}\overline{\mathbf{c}_0^*} + \mathbf{x}_i \cdot (\underline{\mathbf{c}_0^*} - \underline{\mathbf{A}} \cdot \overline{\mathbf{A}}^{-1}\overline{\mathbf{c}_0^*})) \\
&= \sum f_i(\mathsf{id}_i^*)(\mathbf{Y}_i^\top \overline{\mathbf{A}} + \mathbf{x}_i\underline{\mathbf{A}}) \cdot \overline{\mathbf{A}}^{-1}\overline{\mathbf{c}_0^*} + \mathbf{x}_i \cdot (\underline{\mathbf{c}_0^*} - \underline{\mathbf{A}} \cdot \overline{\mathbf{A}}^{-1}\overline{\mathbf{c}_0^*})) \\
&= \sum f_i(\mathsf{id}_i^*)(\mathbf{Y}_i^\top \mid \mathbf{x}_i)\mathbf{c}_0^*
\end{aligned}$$

and $\mathbf{c}_1^*$ is distributed as in G_2. The distribution of K^* can be analyzed with a similar argument. ▌

Initialize:
$\mathbf{A} \xleftarrow{\$} \mathcal{D}_k$
$\varepsilon \xleftarrow{\$} \text{Initialize}_{\mathsf{MAC}}$
For $i = 0, \ldots, \ell$: $\mathbf{Z}_i \xleftarrow{\$} \mathbb{Z}_q^{n \times k}$
For $i = 0, \ldots, \ell'$: $\mathbf{z}'_i \xleftarrow{\$} \mathbb{Z}_q^{1 \times k}$
$\mathsf{pk} := (\mathcal{G}, [\mathbf{A}]_1, ([\mathbf{Z}_i]_1)_{0 \le i \le \ell}, ([\mathbf{z}'_i]_1)_{0 \le i \le \ell'})$
Return pk

USKGen(id):
$\mathcal{Q}_{\mathcal{ID}} = \mathcal{Q}_{\mathcal{ID}} \cup \{\mathsf{id}\}$
$([\mathbf{t}]_2, [u]_2) \xleftarrow{\$} \text{Eval}(\mathsf{id})$
$\mathbf{v}^\top = (\mathbf{t}^\top \sum f_i(\mathsf{id})\mathbf{Z}_i + \sum f'_i(\mathsf{id})\mathbf{z}'_i - u \cdot \underline{\mathbf{A}}) \cdot (\overline{\mathbf{A}})^{-1}$
$\mathsf{usk}[\mathsf{id}] := ([\mathbf{t}]_2, [u]_2, [\mathbf{v}]_2) \in \mathbb{G}_2^n \times \mathbb{G}_2^1 \times \mathbb{G}_2^k$
Return $\mathsf{usk}[\mathsf{id}]$

Enc(id^*): //one query
$([h]_1, [\mathbf{h}_0]_1, [h_1]_T) \xleftarrow{\$} \text{Chal}(\mathsf{id}^*)$
$\overline{\mathbf{c}}_0^* \xleftarrow{\$} \mathbb{Z}_q^k$
$\underline{\mathbf{c}}_0^* = h + \underline{\mathbf{A}} \cdot \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}}_0^* \in \mathbb{Z}_q$
$\mathbf{c}_1^* = \sum_{i=0}^{\ell} f_i(\mathsf{id}^*)\mathbf{Z}_i \cdot \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}}_0^* + \mathbf{h}_0$
$K^* = \sum_{i=0}^{\ell} f_i(\mathsf{id}^*)\mathbf{z}'_i \cdot \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}}_0^* + h_1$
Return $\mathsf{K}^* = [K^*]_T$ and $\mathsf{C}^* = ([\mathbf{c}_0^*]_1, [\mathbf{c}_1^*]_1)$

Finalize(β'):
Return $(\mathsf{id}^* \notin \mathcal{Q}_{\mathcal{ID}}) \wedge \text{Finalize}_{\mathsf{MAC}}(\beta')$

Figure 10: Description of $\mathcal{B}_2$ (having access to the oracles $\text{Initialize}_{\mathsf{MAC}}, \text{Eval}, \text{Chal}, \text{Finalize}_{\mathsf{MAC}}$ of the $\mathsf{PR\text{-}CMA}_{\mathsf{real}}/\mathsf{PR\text{-}CMA}_{\mathsf{rand}}$ games of Figure 1) for the proof of Lemma 4.7.

Lemma 4.7 *There exists an adversary $\mathcal{B}_2$ with $\mathbf{T}(\mathcal{B}_2) \approx \mathbf{T}(\mathcal{A})$ and $\mathsf{Adv}_{\mathsf{MAC}}^{\mathsf{pr\text{-}cma}}(\mathcal{B}_2) \ge |\Pr[\mathsf{G}_4^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathsf{G}_3^{\mathcal{A}} \Rightarrow 1]|$.*

Proof: In G_4, we answer the Enc(id^*) query by choosing random K^* and C^*. We construct an adversary $\mathcal{B}_2$ in Figure 10 to show the differences between G_4 and G_3 can be bounded by the advantage of breaking PR-CMA security of MAC. Intuitively, the reduction to PR-CMA security of the symmetric primitive MAC can be carried out as in both G_3 and G_4, $\mathsf{sk}_{\mathsf{MAC}}$ (i.e., $\mathbf{x}_i$ and x'_i) is perfectly hidden until $\mathcal{B}_2$'s call to Enc(id^*).

If $(\mathbf{h}_0, h_1)$ is uniform (i.e., $\mathcal{B}_2$ is in Game $\mathsf{PR\text{-}CMA}_{\mathsf{rand}}$) then the view of $\mathcal{A}$ is the same as in G_4. If $(\mathbf{h}_0, h_1)$ is real (i.e., $\mathcal{B}_2$ is in Game $\mathsf{PR\text{-}CMA}_{\mathsf{real}}$) then the view of $\mathcal{A}$ is the same as in G_3. ▌

The proof of Theorem 4.3 follows by Lemmas 4.4-4.7 and observing that $\mathsf{G}_4 = \mathsf{PR\text{-}ID\text{-}CPA}_{\mathsf{rand}}$. ▌

5 Hierarchical Identity-based Encryption from Delegatable Affine MACs

In this section, we will define syntax and security requirements of *delegatable* affine MACs and describe our transformation $\mathsf{HIBE}[\mathsf{MAC}, \mathcal{D}_k]$ from delegatable affine MACs to HIBE based on any $\mathcal{D}_k$-MDDH assumption.

5.1 Delegatable Affine MACs

Definition 5.1 An affine MAC over $\mathbb{Z}_q^n$ (Definition 3.1) is *delegatable*, if the message space is $\mathcal{M} = \mathcal{B}^{\le m}$ for some finite base set $\mathcal{B}$, $\ell' = 0$ with $f'_0(\mathsf{m}) = 1$, and there exists a public function $l : \mathcal{M} \to \{0, \ldots, \ell\}$ such that for all $\mathsf{m}' \in \mathcal{M}$ with $\mathsf{m}' = (\mathsf{m}_1, \ldots, \mathsf{m}_{p+1}) \in \mathcal{B}^{p+1}$ and length p prefix $\mathsf{m} = (\mathsf{m}_1, \ldots, \mathsf{m}_p)$ of m, we have $l(\mathsf{m}) \le l(\mathsf{m}')$ and

$$f_i(\mathsf{m}') = \begin{cases} f_i(\mathsf{m}) & 0 \le i \le l(\mathsf{m}) \\ 0 & l(\mathsf{m}') < i \le \ell \end{cases}.$$

Note that for a delegatable MAC, equation (3) simplifies to

$$u = \left(\sum_{i=0}^{l(\mathsf{m})} f_i(\mathsf{m})\mathbf{x}_i^\top + \sum_{i=l(\mathsf{m})+1}^{l(\mathsf{m}')} f_i(\mathsf{m}')\mathbf{x}_i^\top \right) \mathbf{t} + f'_0(\mathsf{m})x'_0.$$

<u>INITIALIZE:</u> $\mathsf{sk}_{\mathsf{MAC}} = (\mathbf{B}, (\mathbf{x}_i)_{0\le i\le \ell}, x_0') \xleftarrow{\$} \mathsf{Gen}_{\mathsf{MAC}}(\mathsf{par})$ Return $([\mathbf{B}]_2, ([\mathbf{x}_i^\top \mathbf{B}]_2)_{0\le i\le\ell})$ <u>EVAL(m):</u> $\mathcal{Q}_{\mathcal{M}} = \mathcal{Q}_{\mathcal{M}} \cup \{\mathsf{m}\}$ $([\mathbf{t}]_2, [u]_2) \xleftarrow{\$} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m})$ For $i = l(\mathsf{m})+1, \dots, \ell$: $d_i = \mathbf{x}_i^\top \mathbf{t} \in \mathbb{Z}_q$ Return $([\mathbf{t}]_2, [u]_2, ([d_i]_2)_{l(\mathsf{m})+1\le i\le\ell})$	<u>CHAL(m*):</u> // one query $h \xleftarrow{\$} \mathbb{Z}_q$ $\mathbf{h}_0 = \sum f_i(\mathsf{m}_i^*)\mathbf{x}_i \cdot h \in \mathbb{Z}_q^n$ $h_1 = x_0' \cdot h \in \mathbb{Z}_q$ $\boxed{h_1 \xleftarrow{\$} \mathbb{Z}_q}$ Return $([h]_1, [\mathbf{h}_0]_1, [h_1]_T)$ <u>FINALIZE($\beta \in \{0,1\}$):</u> Return $\beta \wedge (\mathsf{Prefix}(\mathsf{m}^*) \cap \mathcal{Q}_{\mathcal{M}} = \emptyset)$

Figure 11: Games $\mathsf{HPR\text{-}CMA_{real}}$, and $\boxed{\mathsf{HPR_0\text{-}CMA_{rand}}}$ for defining $\mathsf{HPR_0}$-CMA security.

Intuitively, this property will be used for HIBE user secret key delegation.

SECURITY REQUIREMENTS. Let MAC be a delegatable affine MAC over $\mathbb{Z}_q^n$ with message space $\mathcal{M} = \mathcal{B}^{\le m} := \bigcup_{i=1}^m \mathcal{B}^i$. To build a HIBE, we require a new notion denoted as $\mathsf{HPR_0}$-CMA security. It differs from PR-CMA security in two ways. Firstly, additional values needed for HIBE delegation are provided to the adversary through the call to INITIALIZE and EVAL. Secondly, CHAL always returns a real $\mathbf{h}_0$ which is the reason why our HIBE is not anonymous. (In fact, the additional values actually allow the adversary to distinguish real from random $\mathbf{h}_0$.)

Let $\mathcal{G} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, g_1, g_2, e)$ be an asymmetric pairing group such that $(\mathbb{G}_2, g_2, q)$ is contained in par. Consider the games from Figure 11.

Definition 5.2 A delegatable affine MAC over $\mathbb{Z}_q^n$ is $\mathsf{HPR_0}$-CMA-secure if for all PPT $\mathcal{A}$, $\mathsf{Adv}_{\mathsf{MAC}}^{\mathsf{hpr_0\text{-}cma}}(\mathcal{A}) := \Pr[\mathsf{HPR\text{-}CMA}_{\mathsf{real}}^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathsf{HPR_0\text{-}CMA}_{\mathsf{rand}}^{\mathcal{A}} \Rightarrow 1]$ is negligible.

5.2 An Example of Delegatable Affine MACs

We note that $\mathsf{MAC_{HPS}}[\mathcal{D}_k]$ from Section 3 with message space $\mathcal{M} = \mathcal{B}^{\le m} = (\mathbb{Z}_q^*)^{\le m}$ is delegatable. One should remark the change on $\mathcal{B}$, where we now define $\mathcal{B} = \mathbb{Z}_q^*$ to avoid having a collision between the MAC of m and the MAC of m$\|$0.

Theorem 5.3 *Under the $\mathcal{D}_k$-MDDH assumption, $\mathsf{MAC_{HPS}}[\mathcal{D}_k]$ is $\mathsf{HPR_0}$-CMA-secure. In particular, for all adversaries $\mathcal{A}$ there exists an adversary $\mathcal{D}$ with $\mathbf{T}(\mathcal{A}) \approx \mathbf{T}(\mathcal{D})$ and $\mathsf{Adv}_{\mathsf{MAC_{HPS}}[\mathcal{D}_k]}^{\mathsf{hpr_0\text{-}cma}}(\mathcal{A}) \le 4Q\mathbf{Adv}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{D}) + 2Q/q$, where Q is the maximal number of queries to EVAL$(\cdot)$.*

The proof is postponed to Appendix A.1

5.3 Hierarchical Identity-Based Key Encapsulation

We recall syntax and security of a hierarchical identity-based key encapsulation mechanism (HIBKEM).

Definition 5.4 (Hierarchical Identity-Based Key Encapsulation Mechanism) *A hierarchical identity-based key encapsulation mechanism (HIBE)* HIBKEM *consists of three PPT algorithms* HIBKEM $=$ (Gen, USKDel, , USKGen, Enc, Dec) *with the following properties.*

- *The probabilistic key generation algorithm* $\mathsf{Gen}(1^\lambda)$ *returns the (master) public/secret key and delegation key* (pk, sk, dk)*. Note that for some of our constructions* dk *is empty. We assume that* pk *implicitly defines a hierarchical identity space $\mathcal{ID} = \mathcal{B}^{\le m}$, for some base identity set $\mathcal{B}$, and a key space $\mathcal{K}$, and ciphertext space $\mathcal{C}$.*

- *The probabilistic user secret key generation algorithm* USKGen(sk, id) *returns a secret key* usk[id] *and a delegation value* udk[id] *for hierarchical identity* id $\in \mathcal{ID}$.

Initialize:
 $(\mathsf{pk},\mathsf{sk},\mathsf{dk}) \stackrel{\$}{\leftarrow} \mathsf{Gen}(1^\lambda)$
 Return $(\mathsf{pk},\mathsf{dk})$
 	
 USKGen(id):
 $\mathcal{Q}_{\mathcal{ID}} \leftarrow \mathcal{Q}_{\mathcal{ID}} \cup \{\mathsf{id}\}$
 Return $(\mathsf{usk}[\mathsf{id}],\mathsf{udk}[\mathsf{id}]) \stackrel{\$}{\leftarrow} \mathsf{USKGen}(\mathsf{sk},\mathsf{id})$
	Enc(id*): //one query
	 $(\mathsf{K}^*,\mathsf{C}^*) \stackrel{\$}{\leftarrow} \mathsf{Enc}(\mathsf{pk},\mathsf{id}^*)$
	 $\boxed{\mathsf{K}^* \stackrel{\$}{\leftarrow} \mathcal{K}}$
	 $(\mathsf{K}^*,\mathsf{C}^*) \stackrel{\$}{\leftarrow} \mathcal{K} \times \mathcal{C}$
	 Return $(\mathsf{K}^*,\mathsf{C}^*)$
	
	 Finalize($\beta \in \{0,1\}$):
	 Return $(\mathsf{Prefix}(\mathsf{id}^*) \cap \mathcal{Q}_{\mathcal{ID}} = \emptyset) \wedge \beta$

Figure 12: Games $\mathsf{PR\text{-}HID\text{-}CPA}_{\mathsf{real}}$, $\boxed{\mathsf{IND\text{-}HID\text{-}CPA}_{\mathsf{rand}}}$, and $\mathsf{PR\text{-}HID\text{-}CPA}_{\mathsf{rand}}$ for defining IND-HID-CPA and PR-HID-CPA-security. For any identity $\mathsf{id} \in \mathcal{B}^p$, $\mathsf{Prefix}(\mathsf{id})$ denotes the set of all prefixes of id (where $|\mathsf{Prefix}(\mathsf{id})| = O(|\mathcal{B}|^p)$).

- *The probabilistic key delegation algorithm* $\mathsf{USKDel}(\mathsf{dk},\mathsf{usk}[\mathsf{id}],\mathsf{udk}[\mathsf{id}],\mathsf{id} \in \mathcal{B}^p,\mathsf{id}_{p+1} \in \mathcal{B})$ *returns a user secret key* $\mathsf{usk}[\mathsf{id}|\mathsf{id}_{p+1}]$ *for the hierarchical identity* $\mathsf{id}' = \mathsf{id} \mid \mathsf{id}_{p+1} \in \mathcal{B}^{p+1}$ *and the user delegation key* $\mathsf{udk}[\mathsf{id}']$. *We require* $1 \le |\mathsf{id}| \le m-1$.
- *The probabilistic encapsulation algorithm* $\mathsf{Enc}(\mathsf{pk},\mathsf{id})$ *returns a symmetric key* $\mathsf{K} \in \mathcal{K}$ *together with a ciphertext* C *with respect to the hierarchical identity* $\mathsf{id} \in \mathcal{ID}$.
- *The deterministic decapsulation algorithm* $\mathsf{Dec}(\mathsf{usk}[\mathsf{id}],\mathsf{id},\mathsf{C})$ *returns a decapsulated key* $\mathsf{K} \in \mathcal{K}$ *or the reject symbol* $\perp$.

For correctness we require that for all $\lambda \in \mathbb{N}$, *all pairs* $(\mathsf{pk},\mathsf{sk})$ *generated by* $\mathsf{Gen}(1^\lambda)$, *all* $\mathsf{id} \in \mathcal{ID}$, *all* $\mathsf{usk}[\mathsf{id}]$ *generated by* $\mathsf{USKGen}(\mathsf{sk},\mathsf{id})$ *and all* (K,c) *generated by* $\mathsf{Enc}(\mathsf{pk},\mathsf{id})$*:*

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

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

In our HIBKEM definition we make the delegation key dk and the user delegation key udk[id] explicit to make our constructions more readable. We define indistinguishability (IND-HID-CPA) and pseudorandom ciphertexts (PR-HID-CPA) against adaptively chosen identity and plaintext attacks for a HIBKEM via games $\mathsf{PR\text{-}HID\text{-}CPA}_{\mathsf{real}}$, $\mathsf{IND\text{-}HID\text{-}CPA}_{\mathsf{rand}}$ and $\mathsf{PR\text{-}HID\text{-}CPA}_{\mathsf{rand}}$ from Figure 12.

Definition 5.5 (IND-HID-CPA and PR-HID-CPA Security) *A hierarchical identity-based key encapsulation scheme* HIBKEM *is* IND-HID-CPA*-secure if for all PPT* $\mathcal{A}$, $\mathsf{Adv}^{\mathsf{ind\text{-}hid\text{-}cpa}}_{\mathsf{HIBKEM}}(\mathcal{A}) := |\Pr[\mathsf{PR\text{-}HID\text{-}CPA}^{\mathcal{A}}_{\mathsf{real}} \Rightarrow 1] - \Pr[\mathsf{IND\text{-}HID\text{-}CPA}^{\mathcal{A}}_{\mathsf{rand}}]$ *is negligible. It is* PR-HID-CPA*-secure if for all PPT* $\mathcal{A}$, $\mathsf{Adv}^{\mathsf{pr\text{-}hid\text{-}cpa}}_{\mathsf{HIBKEM}}(\mathcal{A}) := |\Pr[\mathsf{PR\text{-}HID\text{-}CPA}^{\mathcal{A}}_{\mathsf{real}} \Rightarrow 1] - \Pr[\mathsf{PR\text{-}HID\text{-}CPA}^{\mathcal{A}}_{\mathsf{rand}}]$ *is negligible.*

Note that PR-HID-CPA trivially implies IND-HID-CPA and anonymity of HIBKEM.

5.4 The Transformation

Let $\mathcal{D}_k$ be a matrix distribution that outputs matrices $\mathbf{A} \in \mathbb{Z}_q^{(k+1)\times k}$. Let MAC be a delegatable affine MAC over $\mathbb{Z}_q^n$ with message space $\mathcal{M} = \mathcal{B}^{\le m}$. Our $\mathsf{HIBKEM}[\mathsf{MAC},\mathcal{D}_k] = (\mathsf{Gen},\mathsf{USKGen},\mathsf{USKDel},\mathsf{Enc},\mathsf{Dec})$ for key-space $\mathcal{K} = \mathbb{G}_T$ and hierarchical identity space $\mathcal{ID} = \mathcal{M} = \mathcal{B}^{\le m}$ is defined as in Fig. 13. Compared to the IBE construction from Sect. 4, the main difference is that Gen also returns a delegation key dk which allows re-randomization of every usk[id]. Further, USKGen also outputs user delegation keys udk[id] allowing USKDel to delegate.

To show correctness of $\mathsf{HIBKEM}[\mathsf{MAC},\mathcal{D}_k]$, first note that $(\hat{u},\hat{\mathbf{v}})$ computed in USKDel is a correct user secret key for id', $\hat{u} = \sum_{i=0}^{l(\mathsf{id}')} f_i(\mathsf{id}')\mathbf{x}_i^\top\mathbf{t} + x_0'$ and $\hat{\mathbf{v}} = \sum_{i=0}^{l(\mathsf{id}')} f_i(\mathsf{id}')\mathbf{Y}_i\mathbf{t} + \mathbf{y}_0'$. In the next step they get rerandmozied as $u' = \sum_{i=0}^{l(\mathsf{id}')} f_i(\mathsf{id}')\mathbf{x}_i^\top(\mathbf{t} + \mathbf{B}\mathbf{s}')$ and $\mathbf{v}' = \sum_{i=0}^{l(\mathsf{id}')} f_i(\mathsf{id}')\mathbf{Y}_i(\mathbf{t}+\mathbf{B}\mathbf{s}') + \mathbf{y}_0'$. Consequently,

$\underline{\mathsf{Gen}(\mathsf{par}):}$
$\mathbf{A} \xleftarrow{\$} \mathcal{D}_k$
$\mathsf{sk}_{\mathsf{MAC}} = (\mathbf{B}, \mathbf{x}_0, \ldots, \mathbf{x}_\ell, x'_0) \xleftarrow{\$} \mathsf{Gen}_{\mathsf{MAC}}(\mathsf{par})$
For $i = 0, \ldots, \ell$:
$\quad \mathbf{Y}_i \xleftarrow{\$} \mathbb{Z}_q^{k \times n}; \mathbf{Z}_i = (\mathbf{Y}_i^\top \mid \mathbf{x}_i) \cdot \mathbf{A} \in \mathbb{Z}_q^{n \times k}$
$\quad \mathbf{d}_i = \mathbf{x}_i^\top \cdot \mathbf{B} \in \mathbb{Z}_q^{n'}; \mathbf{E}_i = \mathbf{Y}_i \cdot \mathbf{B} \in \mathbb{Z}_q^{k \times n'}$
$\mathbf{y}'_0 \xleftarrow{\$} \mathbb{Z}_q^k; \mathbf{z}'_0 = ({\mathbf{y}'_0}^\top \mid x'_0) \cdot \mathbf{A} \in \mathbb{Z}_q^{1 \times k}$
$\mathsf{pk} := (\mathcal{G}, [\mathbf{A}]_1, ([\mathbf{Z}_i]_1)_{0 \le i \le \ell}, [\mathbf{z}'_0]_1)$
$\mathsf{dk} := ([\mathbf{B}]_2, ([\mathbf{d}_i]_2, [\mathbf{E}_i]_2)_{0 \le i \le \ell})$
$\mathsf{sk} := (\mathsf{sk}_{\mathsf{MAC}}, (\mathbf{Y}_i)_{0 \le i \le \ell}, \mathbf{y}'_0)$
Return $(\mathsf{pk}, \mathsf{dk}, \mathsf{sk})$

$\underline{\mathsf{USKGen}(\mathsf{sk}, \mathsf{id} \in \mathcal{ID}):}$
$([\mathbf{t}]_2, [u]_2) \xleftarrow{\$} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{id})$
$//\ \mathbf{t} \in \mathbb{Z}_q^n; u = \sum f_i(\mathsf{id}) \mathbf{x}_i^\top \mathbf{t} + x'_0 \in \mathbb{Z}_q$
$\mathbf{v} = \sum_{i=0}^{l(\mathsf{id})} f_i(\mathsf{id}) \mathbf{Y}_i \mathbf{t} + \mathbf{y}'_0 \in \mathbb{Z}_q^k$
For $i = l(\mathsf{id}) + 1, \ldots, \ell$:
$\quad d_i = \mathbf{x}_i^\top \mathbf{t} \in \mathbb{Z}_q$
$\quad \mathbf{e}_i = \mathbf{Y}_i \mathbf{t} \in \mathbb{Z}_q^k$
$\mathsf{usk}[\mathsf{id}] := ([\mathbf{t}]_2, [u]_2, [\mathbf{v}]_2) \in \mathbb{G}_2^n \times \mathbb{G}_2^1 \times \mathbb{G}_2^k$
$\mathsf{udk}[\mathsf{id}] := ([d_i]_2, [\mathbf{e}_i]_2)_{l(\mathsf{id}) < i \le \ell} \in (\mathbb{G}_2^{1+k})^{\ell - l(\mathsf{id})}$
Return $(\mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}])$

$\underline{\mathsf{Enc}(\mathsf{pk}, \mathsf{id}):}$
$\mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^k$
$\mathbf{c}_0 = \mathbf{A}\mathbf{r} \in \mathbb{Z}_q^{k+1}$
$\mathbf{c}_1 = (\sum_{i=0}^{l(\mathsf{id})} f_i(\mathsf{id}) \mathbf{Z}_i) \cdot \mathbf{r} \in \mathbb{Z}_q^n$
$K = \mathbf{z}'_0 \cdot \mathbf{r} \in \mathbb{Z}_q$.
Return $\mathsf{K} = [K]_T$ and $\mathsf{C} = ([\mathbf{c}_0]_1, [\mathbf{c}_1]_1)$

$\underline{\mathsf{USKDel}(\mathsf{dk}, \mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}], \mathsf{id} \in \mathcal{B}^p, \mathsf{id}_{p+1} \in \mathcal{B}):}$
If $p \ge m$, then return $\perp$
$\mathsf{id}' := (\mathsf{id}_1, \ldots, \mathsf{id}_p, \mathsf{id}_{p+1}) \in \mathcal{B}^{p+1}$
//Delegation of u and $\mathbf{v}$:
$\hat{u} = u + \sum_{i=l(\mathsf{id})+1}^{l(\mathsf{id}')} f_i(\mathsf{id}') d_i \in \mathbb{Z}_q$
$\hat{\mathbf{v}} = \mathbf{v} + \sum_{i=l(\mathsf{id})+1}^{l(\mathsf{id}')} f_i(\mathsf{id}') \mathbf{e}_i \in \mathbb{Z}_q^k$
//Rerandomization of $\hat{u}$ and $\hat{\mathbf{v}}$:
$\mathbf{s}' \xleftarrow{\$} \mathbb{Z}_q^{n'}$
$\mathbf{t}' = \mathbf{t} + \mathbf{B}\mathbf{s}' \in \mathbb{Z}_q^n$
$u' = \hat{u} + \sum_{i=0}^{l(\mathsf{id}')} f_i(\mathsf{id}') \mathbf{d}_i \mathbf{s}' \in \mathbb{Z}_q$
$\mathbf{v}' = \hat{\mathbf{v}} + \sum_{i=0}^{l(\mathsf{id}')} f_i(\mathsf{id}') \mathbf{E}_i \mathbf{s}' \in \mathbb{Z}_q^k$
//Rerandomization of d'_i and $\mathbf{e}_i$:
For $i = l(\mathsf{id}') + 1, \ldots, \ell$:
$\quad d'_i = d_i + \mathbf{d}_i \mathbf{s}' \in \mathbb{Z}_q$
$\quad \mathbf{e}'_i = \mathbf{e}_i + \mathbf{E}_i \mathbf{s}' \in \mathbb{Z}_q^k$
$\mathsf{usk}[\mathsf{id}'] := ([\mathbf{t}']_2, [u]_2, [\mathbf{v}']_2) \in \mathbb{G}_2^n \times \mathbb{G}_2^1 \times \mathbb{G}_2^k$
$\mathsf{udk}[\mathsf{id}'] := ([d'_i]_2, [\mathbf{e}'_i]_2)_{l(\mathsf{id}') < i \le \ell} \in (\mathbb{G}_2^{1+k})^{\ell - l(\mathsf{id}')}$
Return $(\mathsf{usk}[\mathsf{id}'], \mathsf{udk}[\mathsf{id}'])$

$\underline{\mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id}, \mathsf{C}):}$
Parse $\mathsf{usk}[\mathsf{id}] = ([\mathbf{t}]_2, [u]_2, [\mathbf{v}]_2)$
Parse $\mathsf{C} = ([\mathbf{c}_0]_1, [\mathbf{c}_1]_1)$
$\mathsf{K} = e([\mathbf{c}_0]_1, \begin{bmatrix} \mathbf{v} \\ u \end{bmatrix}_2) - e([\mathbf{c}_1]_1, [\mathbf{t}]_2)$
Return $\mathsf{K} \in \mathbb{G}_T$

Figure 13: Definition of the transformation $\mathsf{HIBKEM}[\mathsf{MAC}, \mathcal{D}_k]$.

$\mathsf{usk}[\mathsf{id}']$ from USKDel has the same distribution as the one output by USKGen. By applying the similar correctness argument from $\mathsf{HIBKEM}[\mathsf{MAC}, \mathcal{D}_k]$, we can show that a correctly generated ciphertext can be correctly decapsulated by using a correct user secret key.

The next theorem shows $\mathsf{IND\text{-}HID\text{-}CPA}$-security of our construction. Its proof is postponed to Appendix B.1. We remark that $\mathsf{HIBKEM}[\mathsf{MAC}, \mathcal{D}_k]$ can never be anonymous as one can always check whether $\mathbf{c}_0 \cdot \sum f_i(\mathsf{id})(\mathbf{E}_i^\top \| \mathbf{d}_i) = c_1 \cdot \mathbf{B}$ using the pairing.

Theorem 5.6 *If* MAC *is* HPR_0-CMA*-secure and the* $\mathcal{D}_k$-MDDH *assumption holds in* $\mathbb{G}_1$ *then* $\mathsf{HIBKEM}[\mathsf{MAC}, \mathcal{D}_k]$ *is* $\mathsf{IND\text{-}HID\text{-}CPA}$ *secure. For all adversaries* $\mathcal{A}$ *there exist adversaries* $\mathcal{B}_1$ *and* $\mathcal{B}_2$ *with* $\mathbf{T}(\mathcal{B}_1) \approx \mathbf{T}(\mathcal{A}) \approx \mathbf{T}(\mathcal{B}_2)$ *and* $\mathsf{Adv}^{\mathsf{ind\text{-}hid\text{-}cpa}}_{\mathsf{HIBKEM}[\mathsf{MAC}, \mathcal{D}_k]}(\mathcal{A}) \le \mathbf{Adv}_{\mathcal{D}_k, \mathsf{GGen}}(\mathcal{B}_1) + \mathsf{Adv}^{\mathsf{hpr_0\text{-}cma}}_{\mathsf{MAC}}(\mathcal{B}_2)$.

5.5 Anonymity-preserving Transformation

In this section, we give an alternative (but less efficient) transformation, which is anonymity-preserving. Our transformation is based on the notion of $\mathsf{APR\text{-}CMA}$-security (anonymity-preserving pseudorandomness against chosen-message attacks) for a delegatable affine MAC MAC over $\mathbb{Z}_q^n$ with message space $\mathcal{M} = \mathcal{B}^{\le m} := \bigcup_{i=1}^m \mathcal{B}^i$. It differs from $\mathsf{HPR\text{-}CMA}$-security (Section 5.1) in the sense that $\textsc{Eval}(\mathsf{m})$ will output the terms required for usk rerandomization, not $\textsc{Initialize}$. Let $\mathcal{G} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, g_1, g_2, e)$ be an asymmetric pairing group such that $(\mathbb{G}_2, g_2, q)$ is contained in par. Consider the games from Figure 14, where the (publicly known) μ is defined as the rank of matrix $\mathbf{B}$ output by $\mathsf{Gen}_{\mathsf{MAC}}(\mathsf{par})$.

<u>INITIALIZE:</u> $\mathsf{sk_{MAC}} = (\mathbf{B}, (\mathbf{x}_i)_{0\le i\le \ell}, \mathbf{x}_0') \stackrel{\$}{\leftarrow} \mathsf{Gen_{MAC}}(\mathsf{par})$ Return ε <u>EVAL(m):</u> $\mathcal{Q}_\mathcal{M} = \mathcal{Q}_\mathcal{M} \cup \{\mathsf{m}\}$ $([\mathbf{t}]_2, [u]_2) \stackrel{\$}{\leftarrow} \mathsf{Tag}(\mathsf{sk_{MAC}}, \mathsf{m})$ $\mathbf{S} \stackrel{\$}{\leftarrow} \mathbb{Z}_q^{n' \times \mu}$; $\mathbf{T} = \mathbf{B} \cdot \mathbf{S} \in \mathbb{Z}_q^{n\times\mu}$ $\mathbf{u} = \sum_{i=0}^{l(\mathsf{m})} f_i(\mathsf{m})\mathbf{x}_i^\top \mathbf{T} \in \mathbb{Z}_q^{1\times\mu}$ For $i = (\mathsf{m}) + 1, \ldots, \ell$: $d_i = \mathbf{x}_i^\top \mathbf{t} \in \mathbb{Z}_q$; $\mathbf{D}_i = \mathbf{x}_i^\top \mathbf{T} \in \mathbb{Z}_q^{1\times\mu}$ Return $([\mathbf{t}]_2, [u]_2, [\mathbf{T}]_2, [\mathbf{u}]_2, ([d_i]_2, [\mathbf{D}_i]_2)_{(\mathsf{m})+1\le i\le \ell})$	<u>CHAL(m*):</u> // one query $h \stackrel{\$}{\leftarrow} \mathbb{Z}_q$ $\mathbf{h}_0 = \sum f_i(\mathsf{m}_i^*)\mathbf{x}_i \cdot h \in \mathbb{Z}_q^n$; $h_1 = x_0' \cdot h \in \mathbb{Z}_q$ $\boxed{(\mathbf{h}_0, h_1) \stackrel{\$}{\leftarrow} \mathbb{Z}_q^n \times \mathbb{Z}_q}$ Return $([h]_1, [\mathbf{h}_0]_1, [h_1]_T)$ <u>FINALIZE($\beta \in \{0,1\}$):</u> Return $\beta \wedge (\mathsf{Prefix}(\mathsf{m}^*) \cap \mathcal{Q}_\mathcal{M} = \emptyset)$

Figure 14: Games $\mathsf{APR\text{-}CMA_{real}}$ and $\boxed{\mathsf{APR\text{-}CMA_{rand}}}$ for defining APR-CMA security.

Definition 5.7 *An affine* MAC *over* $\mathbb{Z}_q^n$ *is* APR-CMA*-secure if for PPT* $\mathcal{A}$*,* $\mathsf{Adv}^{\mathsf{apr\text{-}cma}}_{\mathsf{MAC}}(\mathcal{A}) := \Pr[\mathsf{APR\text{-}CMA}^{\mathcal{A}}_{\mathsf{real}} \Rightarrow 1] - \Pr[\mathsf{APR\text{-}CMA}^{\mathcal{A}}_{\mathsf{rand}} \Rightarrow 1]$ *is negligible.*

Unfortunately, $\mathsf{MAC_{NR}}[\mathcal{D}_k]$ is unlikely to be APR-CMA-secure, since in the security proof the value $\mathbf{u}$ is not pseudorandom and, thus, we can not make $\mathbf{h}_0$ random. The following theorem states that $\mathsf{MAC_{HPS}}[\mathcal{D}_k]$ from Section 3 with message space $\mathcal{M} = \mathcal{B}^{\le m} = (\mathbb{Z}_q^*)^{\le m}$ is anonymous and delegatable.

Theorem 5.8 *Under the* $\mathcal{D}_k$-MDDH *assumption,* $\mathsf{MAC_{HPS}}[\mathcal{D}_k]$ *is* APR-CMA*-secure. In particular, for all adversaries* $\mathcal{A}$ *there exists an adversary* $\mathcal{D}$ *with* $\mathbf{T}(\mathcal{A}) \approx \mathbf{T}(\mathcal{D})$ *and* $\mathsf{Adv}^{\mathsf{apr\text{-}cma}}_{\mathsf{MAC_{HPS}}[\mathcal{D}_k]}(\mathcal{A}) \le 4Q\mathbf{Adv}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{D}) + 2Q/q$*, where* Q *is the maximal number of queries to* EVAL$(\cdot)$*.*

The proof is postponed to Section A.2.

THE ANONYMITY-PRESERVING TRANSFORMATION. Let $\mathcal{D}_k$ be a matrix distribution that outputs matrices $\mathbf{A} \in \mathbb{Z}_q^{(k+1)\times k}$. Let MAC be an delegatable affine MAC over $\mathbb{Z}_q^n$ with message space $\mathcal{M} = \mathcal{B}^{\le m}$. Our $\mathsf{AHIBKEM}[\mathsf{MAC}, \mathcal{D}_k] = (\mathsf{Gen}, \mathsf{USKGen}, \mathsf{USKDel}, \mathsf{Enc}, \mathsf{Dec})$ for key-space $\mathcal{K} = \mathbb{G}_T$ and hierarchical identity space $\mathcal{ID} = \mathcal{M} = \mathcal{B}^{\le m}$ is defined as in Fig. 15. Compared to the HIBE construction from Section 5.4, the new construction uses a different usk rerandomization method: USKGen outputs a random basis $\mathbf{T}$ for vector $\mathbf{t}$ which allows rerandomization of $\mathbf{t}$; similarly, $\mathbf{u}$ and $\mathbf{V}$ are bases for randomizing u and $\mathbf{v}$. Further, Gen will never return $[\mathbf{x}_i^\top \mathbf{B}]_2$ and $[\mathbf{Y}_i\mathbf{B}]_2$, which is the key to preserve anonymity.

Correctness of $\mathsf{AHIBKEM}[\mathsf{MAC}, \mathcal{D}_k]$ follows by the same argument as $\mathsf{HIBKEM}[\mathsf{MAC}, \mathcal{D}_k]$. The following theorem shows PR-HID-CPA security of our construction. Its proof is the same as the one of Theorem 5.6 except that we make the ciphertext to be random based on the APR-CMA security. Details are postponed to Appendix B.2.

Theorem 5.9 *If* MAC *is* APR-CMA*-secure and the* $\mathcal{D}_k$-MDDH *assumption holds in* $\mathbb{G}_1$ *then* $\mathsf{AHIBKEM}[\mathsf{MAC}, \mathcal{D}_k]$ *is* PR-HID-CPA *secure. In particular, for all adversaries* $\mathcal{A}$ *there exist adversaries* $\mathcal{B}_1$ *and* $\mathcal{B}_2$ *with* $\mathbf{T}(\mathcal{B}_1) \approx \mathbf{T}(\mathcal{A}) \approx \mathbf{T}(\mathcal{B}_2)$ *and* $\mathsf{Adv}^{\mathsf{pr\text{-}hid\text{-}cpa}}_{\mathsf{AHIBKEM}[\mathsf{MAC},\mathcal{D}_k]}(\mathcal{A}) \le \mathbf{Adv}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}_1) + \mathsf{Adv}^{\mathsf{apr\text{-}cma}}_{\mathsf{MAC}}(\mathcal{B}_2)$*.*

$\underline{\mathsf{Gen}(\mathsf{par}):}$
$\mathbf{A} \xleftarrow{\$} \mathcal{D}_k$
$\mathsf{sk}_{\mathsf{MAC}} = (\mathbf{B}, \mathbf{x}_0, \ldots, \mathbf{x}_\ell, x_0') \xleftarrow{\$} \mathsf{Gen}_{\mathsf{MAC}}(\mathsf{par})$
For $i = 0, \ldots, \ell$:
$\quad \mathbf{Y}_i \xleftarrow{\$} \mathbb{Z}_q^{k \times n}; \mathbf{Z}_i = (\mathbf{Y}_i^\top \mid \mathbf{x}_i) \cdot \mathbf{A} \in \mathbb{Z}_q^{n \times k}$
$\mathbf{y}_0' \xleftarrow{\$} \mathbb{Z}_q^k; \mathbf{z}_0' = (\mathbf{y}_0'^\top \mid x_0') \cdot \mathbf{A} \in \mathbb{Z}_q^{1 \times k}$
$\mathsf{pk} := (\mathcal{G}, [\mathbf{A}]_1, ([\mathbf{Z}_i]_1)_{0 \le i \le \ell}, [\mathbf{z}_0']_1)$
$\mathsf{sk} := (\mathsf{sk}_{\mathsf{MAC}}, (\mathbf{Y}_i)_{0 \le i \le \ell}, \mathbf{y}_0')$
Return $(\mathsf{pk}, \mathsf{sk})$

$\underline{\mathsf{USKGen}(\mathsf{sk}, \mathsf{id} \in \mathcal{ID}):}$
$([\mathbf{t}]_2, [u]_2) \xleftarrow{\$} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{id})$
$//\ \mathbf{t} \in \mathbb{Z}_q^n; u = \sum f_i(\mathsf{id}) \mathbf{x}_i^\top \mathbf{t} + x_0' \in \mathbb{Z}_q$
$\mathbf{v} = \sum_{i=0}^{l(\mathsf{id})} f_i(\mathsf{id}) \mathbf{Y}_i \mathbf{t} + \mathbf{y}_0' \in \mathbb{Z}_q^k$
$\mathbf{S} \xleftarrow{\$} \mathbb{Z}_q^{n' \times \mu}; \mathbf{T} = \mathbf{B} \cdot \mathbf{S} \in \mathbb{Z}_q^{n \times \mu}$
$\mathbf{u} = \sum_{i=0}^{l(\mathsf{id})} f_i(\mathsf{id}) \mathbf{x}_i^\top \mathbf{T} \in \mathbb{Z}_q^{1 \times \mu}$
$\mathbf{V} = \sum_{i=0}^{l(\mathsf{id})} f_i(\mathsf{id}) \mathbf{Y}_i \mathbf{T} \in \mathbb{Z}_q^{k \times \mu}$
For $i = l(\mathsf{id}) + 1, \ldots, \ell$:
$\quad d_i = \mathbf{x}_i^\top \mathbf{t} \in \mathbb{Z}_q; \mathbf{D}_i = \mathbf{x}_i^\top \mathbf{T} \in \mathbb{Z}_q^{1 \times \mu}$
$\quad \mathbf{e}_i = \mathbf{Y}_i \mathbf{t} \in \mathbb{Z}_q^k; \mathbf{E}_i = \mathbf{Y}_i \mathbf{T} \in \mathbb{Z}_q^{k \times \mu}$
$\mathsf{usk}[\mathsf{id}] := ([\mathbf{t}]_2, [u]_2, [\mathbf{v}]_2) \in \mathbb{G}_2^n \times \mathbb{G}_2^1 \times \mathbb{G}_2^k$
$\mathsf{udk}[\mathsf{id}] := ([\mathbf{T}]_2, [\mathbf{u}]_2, [\mathbf{V}]_2, ([d_i]_2, [\mathbf{D}_i]_2, [\mathbf{e}_i]_2, [\mathbf{E}_i]_2)_{l(\mathsf{id}) < i \le \ell})$
$\quad \in \mathbb{G}_2^{n \times \mu} \times \mathbb{G}_2^{1 \times \mu} \times \mathbb{G}_2^{k \times \mu} \times (\mathbb{G}_2 \times \mathbb{G}_2^{1 \times \mu} \times \mathbb{G}_2^k \times \mathbb{G}_2^{k \times \mu})^{\ell - l(\mathsf{id})}$
Return $(\mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}])$

$\underline{\mathsf{Enc}(\mathsf{pk}, \mathsf{id}):}$
$\mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^k$
$\mathbf{c}_0 = \mathbf{A}\mathbf{r} \in \mathbb{Z}_q^{k+1}$
$\mathbf{c}_1 = (\sum_{i=0}^{l(\mathsf{id})} f_i(\mathsf{id}) \mathbf{Z}_i) \cdot \mathbf{r} \in \mathbb{Z}_q^n$
$K = \mathbf{z}_0' \cdot \mathbf{r} \in \mathbb{Z}_q$.
Return $\mathsf{K} = [K]_T$ and $\mathsf{C} = ([\mathbf{c}_0]_1, [\mathbf{c}_1]_1)$

$\underline{\mathsf{USKDel}(\mathsf{dk}, \mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}], \mathsf{id} \in \mathcal{B}^p, \mathsf{id}_{p+1} \in \mathcal{B}):}$
If $p \ge m$, then return $\perp$
$\mathsf{id}' := (\mathsf{id}_1, \ldots, \mathsf{id}_p, \mathsf{id}_{p+1}) \in \mathcal{B}^{p+1}$
//Delegation of $(u, \mathbf{v})$ and $(\mathbf{u}, \mathbf{V})$:
$\hat{u} = u + \sum_{i=l(\mathsf{id})+1}^{l(\mathsf{id}')} f_i(\mathsf{id}') d_i \in \mathbb{Z}_q$
$\hat{\mathbf{v}} = \mathbf{v} + \sum_{i=l(\mathsf{id})+1}^{l(\mathsf{id}')} f_i(\mathsf{id}') \mathbf{e}_i \in \mathbb{Z}_q^k$
$\hat{\mathbf{u}} = \mathbf{u} + \sum_{i=l(\mathsf{id})+1}^{l(\mathsf{id}')} f_i(\mathsf{id}') \mathbf{D}_i \in \mathbb{Z}_q^{1 \times \mu}$
$\hat{\mathbf{V}} = \mathbf{V} + \sum_{i=l(\mathsf{id})+1}^{l(\mathsf{id}')} f_i(\mathsf{id}') \mathbf{E}_i \in \mathbb{Z}_q^{k \times \mu}$
//Rerandomization of $(\hat{u}, \hat{\mathbf{v}})$ and $(\hat{\mathbf{u}}, \hat{\mathbf{V}})$:
$\mathbf{s}' \xleftarrow{\$} \mathbb{Z}_q^\mu$; $\mathbf{S} \xleftarrow{\$} \mathbb{Z}_q^{\mu \times \mu}$
$\mathbf{t}' = \mathbf{t} + \mathbf{T}\mathbf{s}' \in \mathbb{Z}_q^n$; $\mathbf{T}' = \hat{\mathbf{T}} \cdot \mathbf{S}' \in \mathbb{Z}_q^{n \times \mu}$
$u' = \hat{u} + \hat{\mathbf{u}} \cdot \mathbf{s}' \in \mathbb{Z}_q$; $\mathbf{u}' = \hat{\mathbf{u}} \cdot \mathbf{S}' \in \mathbb{Z}_q^{1 \times \mu}$
$\mathbf{v}' = \hat{\mathbf{v}} + \hat{\mathbf{V}} \cdot \mathbf{s}' \in \mathbb{Z}_q^k$; $\mathbf{V}' = \hat{\mathbf{V}} \cdot \mathbf{S}' \in \mathbb{Z}_q^{k \times \mu}$
//Rerandomization of d_i' and $\mathbf{e}_i$:
For $i = l(\mathsf{id}') + 1, \ldots, \ell$:
$\quad d_i' = d_i + \mathbf{D}_i \mathbf{s}' \in \mathbb{Z}_q$; $\mathbf{D}_i' = \mathbf{D}_i \cdot \mathbf{S}' \in \mathbb{Z}_q^{1 \times \mu}$
$\quad \mathbf{e}_i' = \mathbf{e}_i + \mathbf{E}_i \mathbf{s}' \in \mathbb{Z}_q^k$; $\mathbf{E}_i' = \mathbf{E}_i \cdot \mathbf{S}' \in \mathbb{Z}_q^{k \times \mu}$
$\mathsf{usk}[\mathsf{id}'] := ([\mathbf{t}']_2, [u']_2, [\mathbf{v}']_2)$
$\mathsf{udk}[\mathsf{id}'] := ([\mathbf{T}']_2, [\mathbf{u}']_2, [\mathbf{V}']_2, ([d_i']_2, [\mathbf{D}_i']_2, [\mathbf{e}_i']_2,$
$[\mathbf{E}_i']_2)_{l(\mathsf{id}') < i \le \ell})$
Return $(\mathsf{usk}[\mathsf{id}'], \mathsf{udk}[\mathsf{id}'])$

$\underline{\mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id}, \mathsf{C}):}$
Parse $\mathsf{usk}[\mathsf{id}] = ([\mathbf{t}]_2, [u]_2, [\mathbf{v}]_2)$
Parse $\mathsf{C} = ([\mathbf{c}_0]_1, [\mathbf{c}_1]_1)$
$\mathsf{K} = e([\mathbf{c}_0]_1, \begin{bmatrix} \mathbf{v} \\ u \end{bmatrix}_2) - e([\mathbf{c}_1]_1, [\mathbf{t}]_2)$
Return $\mathsf{K} \in \mathbb{G}_T$

Figure 15: Definition of the transformation $\mathsf{AHIBKEM}[\mathsf{MAC}, \mathcal{D}_k]$. μ denotes the rank of $\mathbf{B}$.

Acknowledgements

We thank Hoeteck Wee and Jie Chen for comments and helpful discussions. All authors were (partially) funded by a Sofja Kovalevskaja Award of the Alexander von Humboldt Foundation. Eike Kiltz was partially funded by ERC Project ERCC (FP7/615074). Jiaxin Pan was partially funded by the German Israeli Foundation.

References

[1] J. Alwen, Y. Dodis, M. Naor, G. Segev, S. Walfish, and D. Wichs. Public-key encryption in the bounded-retrieval model. In H. Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 113–134. Springer, Heidelberg, May 2010. (Cited on page 30.)

[2] M. Bellare and S. Goldwasser. New paradigms for digital signatures and message authentication based on non-interative zero knowledge proofs. In G. Brassard, editor, *CRYPTO'89*, volume 435 of *LNCS*, pages 194–211. Springer, Heidelberg, Aug. 1990. (Cited on page 1, 3.)

[3] M. Bellare and T. Ristenpart. Simulation without the artificial abort: Simplified proof and improved concrete security for Waters' IBE scheme. In A. Joux, editor, *EUROCRYPT 2009*, volume 5479 of *LNCS*, pages 407–424. Springer, Heidelberg, Apr. 2009. (Cited on page 34.)

[4] O. Blazy, S. A. Kakvi, E. Kiltz, and J. Pan. Tightly-secure signatures from chameleon hash functions. In J. Katz, editor, *PKC 2015*, volume 9020 of *LNCS*, pages 256–279. Springer, Heidelberg, Mar. / Apr. 2015. (Cited on page 3.)

[5] O. Blazy, E. Kiltz, and J. Pan. (Hierarchical) identity-based encryption from affine message authentication. In J. A. Garay and R. Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 408–425. Springer, Heidelberg, Aug. 2014. (Cited on page 5.)

[6] D. Boneh and M. K. Franklin. Identity-based encryption from the Weil pairing. In J. Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 213–229. Springer, Heidelberg, Aug. 2001. (Cited on page 1.)

[7] J. Chen, H. W. Lim, S. Ling, H. Wang, and H. Wee. Shorter IBE and signatures via asymmetric pairings. In M. Abdalla and T. Lange, editors, *PAIRING 2012*, volume 7708 of *LNCS*, pages 122–140. Springer, Heidelberg, May 2013. (Cited on page 3.)

[8] J. Chen and H. Wee. Fully, (almost) tightly secure IBE and dual system groups. In R. Canetti and J. A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 435–460. Springer, Heidelberg, Aug. 2013. (Cited on page 1, 2, 3, 4, 7, 8.)

[9] C. Cocks. An identity based encryption scheme based on quadratic residues. In B. Honary, editor, *8th IMA International Conference on Cryptography and Coding*, volume 2260 of *LNCS*, pages 360–363. Springer, Heidelberg, Dec. 2001. (Cited on page 1.)

[10] R. Cramer and V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In H. Krawczyk, editor, *CRYPTO'98*, volume 1462 of *LNCS*, pages 13–25. Springer, Heidelberg, Aug. 1998. (Cited on page 4.)

[11] R. Cramer and V. Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In L. R. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 45–64. Springer, Heidelberg, Apr. / May 2002. (Cited on page 1.)

[12] Y. Dodis, E. Kiltz, K. Pietrzak, and D. Wichs. Message authentication, revisited. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 355–374. Springer, Heidelberg, Apr. 2012. (Cited on page 2, 3, 7, 10.)

[13] A. Escala, G. Herold, E. Kiltz, C. Ràfols, and J. Villar. An algebraic framework for Diffie-Hellman assumptions. In R. Canetti and J. A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 129–147. Springer, Heidelberg, Aug. 2013. (Cited on page 2, 3, 5, 6, 10.)

[14] C. Gentry and A. Silverberg. Hierarchical ID-based cryptography. In Y. Zheng, editor, *ASIACRYPT 2002*, volume 2501 of *LNCS*, pages 548–566. Springer, Heidelberg, Dec. 2002. (Cited on page 3.)

[15] J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In N. P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 415–432. Springer, Heidelberg, Apr. 2008. (Cited on page 4.)

[16] D. Hofheinz and T. Jager. Tightly secure signatures and public-key encryption. In R. Safavi-Naini and R. Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 590–607. Springer, Heidelberg, Aug. 2012. (Cited on page 3.)

[17] C. S. Jutla and A. Roy. Shorter quasi-adaptive NIZK proofs for linear subspaces. In K. Sako and P. Sarkar, editors, *ASIACRYPT 2013, Part I*, volume 8269 of *LNCS*, pages 1–20. Springer, Heidelberg, Dec. 2013. (Cited on page 3, 4.)

[18] E. Kiltz and G. Neven. Identity-based signatures. In M. Joye and G. Neven, editors, *Identity-Based Cryptography*. IOS Press, 2009. (Cited on page 3.)

[19] E. Kiltz, J. Pan, and H. Wee. Structure-preserving signatures from standard assumptions, revisited. In R. Gennaro and M. J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 275–295. Springer, Heidelberg, Aug. 2015. (Cited on page 3.)

[20] E. Kiltz, K. Pietrzak, M. Stam, and M. Yung. A new randomness extraction paradigm for hybrid encryption. In A. Joux, editor, *EUROCRYPT 2009*, volume 5479 of *LNCS*, pages 590–609. Springer, Heidelberg, Apr. 2009. (Cited on page 3, 30.)

[21] E. Kiltz and H. Wee. Quasi-adaptive NIZK for linear subspaces revisited. In E. Oswald and M. Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 101–128. Springer, Heidelberg, Apr. 2015. (Cited on page 3.)

[22] A. B. Lewko. Tools for simulating features of composite order bilinear groups in the prime order setting. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 318–335. Springer, Heidelberg, Apr. 2012. (Cited on page 3.)

[23] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In H. Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 62–91. Springer, Heidelberg, May 2010. (Cited on page 4.)

[24] A. B. Lewko and B. Waters. New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In D. Micciancio, editor, *TCC 2010*, volume 5978 of *LNCS*, pages 455–479. Springer, Heidelberg, Feb. 2010. (Cited on page 4.)

[25] M. Naor and O. Reingold. Number-theoretic constructions of efficient pseudo-random functions. In *38th FOCS*, pages 458–467. IEEE Computer Society Press, Oct. 1997. (Cited on page 2.)

[26] M. Naor and O. Reingold. On the construction of pseudo-random permutations: Luby-Rackoff revisited (extended abstract). In *29th ACM STOC*, pages 189–199. ACM Press, May 1997. (Cited on page 8.)

[27] R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairing. In *SCIS 2000*, Okinawa, Japan, Jan. 2000. (Cited on page 1.)

[28] A. Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and D. Chaum, editors, *CRYPTO'84*, volume 196 of *LNCS*, pages 47–53. Springer, Heidelberg, Aug. 1984. (Cited on page 1.)

[29] B. Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In S. Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 619–636. Springer, Heidelberg, Aug. 2009. (Cited on page 1, 3, 4.)

[30] B. R. Waters. Efficient identity-based encryption without random oracles. In R. Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 114–127. Springer, Heidelberg, May 2005. (Cited on page 1, 3, 34.)

[31] H. Wee. Dual system encryption via predicate encodings. In Y. Lindell, editor, *TCC 2014*, volume 8349 of *LNCS*, pages 616–637. Springer, Heidelberg, Feb. 2014. (Cited on page 4.)

A Security Proofs for the MACs

A.1 Security of Delegatable $\mathsf{MAC}_{\mathsf{HPS}}[\mathcal{D}_k]$ (Theorem 5.3)

We prove Theorem 5.3 by defining a sequence of intermediate games G_0-G_2 as in Figure 16.

Lemma A.1 $\Pr[\mathsf{HPR\text{-}CMA}^{\mathcal{A}}_{\mathsf{real}} \Rightarrow 1] = \Pr[\mathsf{G}_0^{\mathcal{A}} \Rightarrow 1]$

$\underline{\text{INITIALIZE:}}$ // Games G_0-G_2
$\mathbf{B} \xleftarrow{\$} \mathcal{D}_k$; $x_0' \leftarrow_\$ \mathbb{Z}_q$
For $j = 0, \dots, m : \mathbf{x}_j \leftarrow_\$ \mathbb{Z}_q^{k+1}$
Return $([\mathbf{B}]_2, ([\mathbf{x}_j^\top \mathbf{B}]_2)_{0 \le j \le m})$

$\underline{\text{CHAL}(\mathsf{m}^*)\text{:}}$ //Games G_0-$\mathsf{G}_{1,Q+1}$, $\boxed{\mathsf{G}_2}$
$h \xleftarrow{\$} \mathbb{Z}_q$
$\mathbf{h}_0 = (\mathbf{x_0}^\top + \sum \mathsf{m}_i^* \cdot \mathbf{x}_i^\top)h \in \mathbb{Z}_q^{k+1}$
$h_1 = x_0' h \in \mathbb{Z}_q$, $\boxed{h_1 \xleftarrow{\$} \mathbb{Z}_q}$
Return $([h]_1, [\mathbf{h}_0]_1, [h_1]_T)$

$\underline{\text{FINALIZE}(d \in \{0,1\})\text{:}}$ // Games G_0-G_2
Return $(\mathsf{Prefix}(\mathsf{m}^*) \cap \mathcal{Q}_\mathcal{M} = \emptyset) \wedge d$.

$\underline{\text{EVAL}(\mathsf{m})\text{:}}$ // Games G_2
$\mathcal{Q}_\mathcal{M} = \mathcal{Q}_\mathcal{M} \cup \{\mathsf{m}\}$
$(\mathbf{t}, u) \xleftarrow{\$} \mathbb{Z}_q^{k+1} \times \mathbb{Z}_q$
For $j = |\mathsf{m}| + 1, \dots, m$: $d_j = \mathbf{x}_j^\top \mathbf{t}$
Return $([\mathbf{t}]_2, [u]_2, ([d_j]_2)_{|\mathsf{m}| < j \le m})$

$\underline{\text{EVAL}(\mathsf{m})\text{:}}$ // Games G_0
$\mathcal{Q}_\mathcal{M} = \mathcal{Q}_\mathcal{M} \cup \{\mathsf{m}\}$
$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k, \mathbf{t} = \mathbf{Bs}$
$u = (\mathbf{x}_0^\top + \sum_{j=1}^{|\mathsf{m}|} \mathsf{m}_j \cdot \mathbf{x}_j^\top)\mathbf{t} + x_0'$
For $|\mathsf{m}| < j \le m$: $d_j = \mathbf{x}_j^\top \mathbf{t}$
Return $([\mathbf{t}]_2, [u]_2, ([d_j]_2)_{|\mathsf{m}| < j \le m})$

$\underline{\text{EVAL}(\mathsf{m})\text{:}}$ //Games $\mathsf{G}_{1,i}$, $\boxed{\mathsf{G}_{1.1,i}\text{-}\mathsf{G}_{1.2,i}}$, $\mathsf{G}_{1.2,i}$-$\mathsf{G}_{1.3,i}$, $\mathsf{G}_{1.3,i}$
$\mathcal{Q}_\mathcal{M} = \mathcal{Q}_\mathcal{M} \cup \{\mathsf{m}\}$ //Let m be the c-th query $(1 \le c \le Q)$
$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{t} = \mathbf{Bs}$
If $c < i$ then $u \xleftarrow{\$} \mathbb{Z}_q$
If $c > i$ then $u = (\mathbf{x}_0^\top + \sum_{j=1}^{|\mathsf{m}|} \mathsf{m}_j \cdot \mathbf{x}_j^\top)\mathbf{t} + x_0'$
If $c = i$ then
$\boxed{\mathbf{t} \xleftarrow{\$} \mathbb{Z}_q^{k+1}}$; $\mathbf{t} = \mathbf{Bs}$
$u = (\mathbf{x}_0^\top + \sum_{j=1}^{|\mathsf{m}|} \mathsf{m}_j \cdot \mathbf{x}_j^\top)\mathbf{t} + x_0'$; $u \xleftarrow{\$} \mathbb{Z}_q$
For $j = |\mathsf{m}| + 1, \dots, m$: $d_j = \mathbf{x}_j^\top \mathbf{t}$
Return $([\mathbf{t}]_2, [u]_2, ([d_j]_2)_{|\mathsf{m}| < j \le m})$

Figure 16: Games G_0 to G_2 for the proof of Theorem 5.3.

Similar to the proof of Theorem 3.9, we define the game $\mathsf{G}_{1,i}$. Different to Theorem 3.9, we always honestly compute $\mathbf{t} = \mathbf{Bs}$ in $\mathsf{G}_{1,i}$, otherwise, too much information about $\mathbf{x}_j$ will be leaked from terms $[d_j]_2$. To interpolate between $\mathsf{G}_{1,i}$ and $\mathsf{G}_{1,i+1}$, we also define $\mathsf{G}_{1.1,i}$ to $\mathsf{G}_{1.3,i}$.

By the same arguments as in Section 3.3, we have the following two lemmas:

Lemma A.2 $\Pr[\mathsf{G}_0^\mathcal{A} \Rightarrow 1] = \Pr[\mathsf{G}_{1,1}^\mathcal{A} \Rightarrow 1]$

Lemma A.3 *There exists an adversary $\mathcal{D}$ with $\mathbf{T}(\mathcal{D}) \approx \mathbf{T}(\mathcal{A})$ and $\mathbf{Adv}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{D}) \ge |\Pr[\mathsf{G}_{1.1,i}^\mathcal{A} \Rightarrow 1] - \Pr[\mathsf{G}_{1,i}^\mathcal{A} \Rightarrow 1]|$.*

Lemma A.4 $|\Pr[\mathsf{G}_{1.2,i}^\mathcal{A} \Rightarrow 1] - \Pr[\mathsf{G}_{1.1,i}^\mathcal{A} \Rightarrow 1]| \le 1/q$.

Proof: At a high level, those two games are only separated by the 2-universality of the underlying hash proof system. The following arguments are similar to Lemma 3.12. Let m the i-th queried message. We have $\mathsf{m} \neq \mathsf{m}^*$ and let i' be the smallest index such that $\mathsf{m}_{i'} \neq \mathsf{m}_{i'}^*$, where $\mathsf{m}_{i'}$ (resp. $\mathsf{m}_{i'}^*$) denotes the i'-th entry of m (resp. m^*). By the definition of HPR_0-CMA security, m can not be a prefix of m^*. Thus, either ($i' \le |\mathsf{m}^*|$ and $i' \le |\mathsf{m}|$), which leads to the same information-theoretical argument as in Lemma 3.12, or $i' \ge |\mathsf{m}^*| + 1$ and $\mathsf{m}_j^* = \mathsf{m}_j$ for all $j \le |\mathsf{m}^*|$. In the latter case, $\mathcal{A}$ obtains the following equations in the unknown variables $\mathbf{x}_0, \mathbf{x}_{i'}$ in an information-theoretical way:

$$\begin{pmatrix} \mathbf{B}^\top \mathbf{x}_0 \\ \mathbf{B}^\top \mathbf{x}_{i'} \\ \mathbf{h}_0 \\ u - x_0' \end{pmatrix} = \underbrace{\begin{pmatrix} \mathbf{B}^\top & \mathbf{0} \\ \mathbf{0} & \mathbf{B}^\top \\ h \cdot \mathbf{I}_{k+1} & \mathbf{0} \\ \mathbf{t}^\top & \mathsf{m}_{i'} \mathbf{t}^\top \end{pmatrix}}_{=:\mathbf{M}} \cdot \begin{pmatrix} \mathbf{x}_0 \\ \mathbf{x}_{i'} \end{pmatrix},$$

where $\mathbf{B}^\top \mathbf{x}_0$ and $\mathbf{B}^\top \mathbf{x}_{i'}$ are from INITIALIZE and c-th EVAL queries ($c \neq i$), $\mathbf{h}_0$ is from $\text{CHAL}(\mathsf{m}^*)$, and $u - x_0'$ is from $\text{EVAL}(\mathsf{m})$. $\mathbf{I}_{k+1}$ denotes the $(k+1) \times (k+1)$ identity matrix. We note that the terms $[d_{i'}]_2$ from the c-th EVAL queries ($c \neq i$) only leak the information about $\mathbf{x}_{i'}$ on the span of $\mathbf{B}$.

As shown in Lemma 3.12, the last row of $\mathbf{M} \in \mathbb{Z}_q^{(3k+2) \times (2k+2)}$ is linearly independent of the first $2k$ rows (except with probability $1/q$). Also, the last row is linearly independent of rows $2k+1$ to $3k+1$. Thus,

$u - x_0'$ is linearly independent of $\mathbf{B}^\top \mathbf{x}_0$, $\mathbf{B}^\top \mathbf{x}_{i'}$ and $\mathbf{h}_0$ and therefore u is distributed uniformly at random in $\mathsf{G}'_{1,i}$. ▌

We have the following two straightforward lemmas.

Lemma A.5 *There exists an adversary* $\mathcal{D}$ *with* $\mathbf{T}(\mathcal{D}) \approx \mathbf{T}(\mathcal{A})$ *and* $\mathbf{Adv}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{D}) \geq |\Pr[\mathsf{G}^{\mathcal{A}}_{1.3,i} \Rightarrow 1] - \Pr[\mathsf{G}^{\mathcal{A}}_{1.2,i} \Rightarrow 1]|$.

Lemma A.6 $\Pr[\mathsf{G}^{\mathcal{A}}_{1.3,i} \Rightarrow 1] = \Pr[\mathsf{G}^{\mathcal{A}}_{1,i+1} \Rightarrow 1]$

Lemma A.7 $\Pr[\mathsf{G}^{\mathcal{A}}_{2} \Rightarrow 1] = \Pr[\mathsf{G}^{\mathcal{A}}_{1,Q+1} \Rightarrow 1]$.

Proof: In G_2, we replace h_1 output by $\textsc{Chal}(\mathsf{m}^*, c)$ with a random value. Similar to Lemma 3.13, since all the answers of $\textsc{Eval}$ are independent of x_0' (in particular, u is uniformly random), h_1 is uniformly random in the view of $\mathcal{A}$. ▌

We apply all the arguments before in a reverse order and then we easily get the following:

Lemma A.8 *There exists an adversary* $\mathcal{D}$ *with* $\mathbf{T}(\mathcal{D}) \approx \mathbf{T}(\mathcal{A})$ *and* $|\Pr[\mathsf{HPR_0\text{-}CMA}^{\mathcal{A}}_{\mathsf{rand}} \Rightarrow 1] - \Pr[\mathsf{G}^{\mathcal{A}}_{2} \Rightarrow 1]| \leq Q(2\mathbf{Adv}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{D}) + 1/q)$.

The proof of the theorem follows by combining Lemmas A.1-A.8.

A.2 Anonymity of delegatable $\mathsf{MAC_{HPS}}[\mathcal{D}_k]$ (Theorem 5.8)

We prove Theorem 5.8 by defining a sequence of intermediate games as in Figure 17. Let $\mathcal{A}$ be an adversary against the $\mathsf{APR\text{-}CMA}$-security of $\mathsf{MAC_{HPS}}[\mathcal{D}_k]$.

<u>$\textsc{Initialize}$:</u> // Games G_0-G_2
$\mathbf{B} \xleftarrow{\$} \mathcal{D}_k$; $x_0' \leftarrow_\$ \mathbb{Z}_q$
For $j = 0, \ldots, \ell : \mathbf{x}_j \leftarrow_\$ \mathbb{Z}_q^{k+1}$
Return ε

<u>$\textsc{Chal}(\mathsf{m}^*)$:</u> //Games G_0-$\mathsf{G}_{1,Q+1}$, $\boxed{\mathsf{G}_2}$
$h \xleftarrow{\$} \mathbb{Z}_q$
$\mathbf{h}_0 = (\mathbf{x_0} + \sum \mathsf{m}_j^* \cdot \mathbf{x}_j)h \in \mathbb{Z}_q^{k+1}$; $\boxed{\mathbf{h}_0 \xleftarrow{\$} \mathbb{Z}_q^{k+1}}$
$h_1 = x_0' h \in \mathbb{Z}_q$; $\boxed{h_1 \xleftarrow{\$} \mathbb{Z}_q}$
Return $([h]_1, [\mathbf{h}_0]_1, [h_1]_T)$

<u>$\textsc{Finalize}(d \in \{0,1\})$:</u> // Games G_0-G_2
Return $d \wedge (\mathsf{Prefix}(\mathsf{m}^*) \cap \mathcal{Q}_{\mathcal{M}} = \emptyset)$

<u>$\textsc{Eval}(\mathsf{m})$:</u> //Game G_2
$\mathcal{Q}_{\mathcal{M}} = \mathcal{Q}_{\mathcal{M}} \cup \{\mathsf{m}\}$
$(\mathbf{t}, u) \xleftarrow{\$} \mathbb{Z}_q^{k+1} \times \mathbb{Z}_q$
$(\mathbf{T}, \mathbf{u}) \xleftarrow{\$} \mathbb{Z}_q^{(k+1)\times k} \times \mathbb{Z}_q^{1\times k}$
For $j = |\mathsf{m}|+1, \ldots, m : d_i = \mathbf{x}_i^\top \mathbf{t}$; $\mathbf{D}_i = \mathbf{x}_i^\top \mathbf{T}$
Return $([\mathbf{t}]_2, [u]_2, [\mathbf{T}]_2, [\mathbf{u}]_2, ([d_j]_2, [\mathbf{D}_j]_2)_{|\mathsf{m}|<j\leq m})$

<u>$\textsc{Eval}(\mathsf{m})$:</u> // Games G_0
$\mathcal{Q}_{\mathcal{M}} = \mathcal{Q}_{\mathcal{M}} \cup \{\mathsf{m}\}$
$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k, \mathbf{t} = \mathbf{B}\mathbf{s} \in \mathbb{Z}_q^{k+1}$
$u = (\mathbf{x}_0^\top + \sum_{j=1}^{|\mathsf{m}|} \mathsf{m}_j \cdot \mathbf{x}_j^\top)\mathbf{t} + x_0' \in \mathbb{Z}_q$
$\mathbf{S} \xleftarrow{\$} \mathbb{Z}_q^{k\times k}$; $\mathbf{T} = \mathbf{B} \cdot \mathbf{S} \in \mathbb{Z}_q^{(k+1)\times k}$
$\mathbf{u} = (\mathbf{x}_0^\top + \sum \mathsf{m}_j \mathbf{x}_j^\top)\mathbf{T} \in \mathbb{Z}_q^{1\times k}$
For $|\mathsf{m}| < j \leq m$: $d_j = \mathbf{x}_j^\top \mathbf{t} \in \mathbb{Z}_q$; $\mathbf{D}_j = \mathbf{x}_j^\top \mathbf{T} \in \mathbb{Z}_q^{1\times k}$
Return $([\mathbf{t}]_2, [u]_2, [\mathbf{T}]_2, [\mathbf{u}]_2, ([d_j]_2, [\mathbf{D}_j]_2)_{|\mathsf{m}|<j\leq m})$

<u>$\textsc{Eval}(\mathsf{m})$:</u> //Games $\mathsf{G}_{1,i}$, $\boxed{\mathsf{G}_{1.1,i}\text{-}\mathsf{G}_{1.2,i}}$, $\boxed{\mathsf{G}_{1.2,i}\text{-}\mathsf{G}_{1.3,i}}$, $\mathsf{G}_{1.3,i}$
$\mathcal{Q}_{\mathcal{M}} = \mathcal{Q}_{\mathcal{M}} \cup \{\mathsf{m}\}$ //Let m be the c-th query $(1 \leq c \leq Q)$
$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k, \mathbf{t} = \mathbf{B}\mathbf{s} \in \mathbb{Z}_q^{k+1}$; $\mathbf{S} \xleftarrow{\$} \mathbb{Z}_q^{k\times k}$; $\mathbf{T} = \mathbf{B} \cdot \mathbf{S} \in \mathbb{Z}_q^{(k+1)\times k}$
If $c < i$ then
  $u \xleftarrow{\$} \mathbb{Z}_q$; $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^{1\times k}$
If $c > i$ then
  $u = (\mathbf{x}_0^\top + \sum_{j=1}^{|\mathsf{m}|} \mathsf{m}_j \cdot \mathbf{x}_j^\top)\mathbf{t} + x_0'$
  $\mathbf{u} = (\mathbf{x}_0^\top + \sum \mathsf{m}_j \mathbf{x}_j^\top)\mathbf{T}$
If $c = i$ then
  $\boxed{\mathbf{t} \xleftarrow{\$} \mathbb{Z}_q^{k+1}}$; $\mathbf{t} = \mathbf{B}\mathbf{s}$
  $u = (\mathbf{x}_0^\top + \sum_{j=1}^{|\mathsf{m}|} \mathsf{m}_j \cdot \mathbf{x}_j^\top)\mathbf{t} + x_0'$; $\boxed{u \xleftarrow{\$} \mathbb{Z}_q}$
  $\boxed{\mathbf{T} \xleftarrow{\$} \mathbb{Z}_q^{(k+1)\times k}}$; $\mathbf{T} = \mathbf{B}\mathbf{S}$
  $\mathbf{u} = (\mathbf{x}_0^\top + \sum \mathsf{m}_j \mathbf{x}_j^\top)\mathbf{T}$; $\boxed{\mathbf{u} \xleftarrow{\$} \mathbb{Z}_q^{1\times k}}$
For $j = |\mathsf{m}|+1, \ldots, m$: $d_j = \mathbf{x}_j^\top \mathbf{t}$; $\mathbf{D}_j = \mathbf{x}_j^\top \mathbf{T}$
Return $([\mathbf{t}]_2, [u]_2, [\mathbf{T}]_2, [\mathbf{u}]_2, ([d_j]_2, [\mathbf{D}_j]_2)_{|\mathsf{m}|<j\leq m})$

Figure 17: Games $\mathsf{G}_0, (\mathsf{G}_{1,i}, \mathsf{G}'_{1,i})_{1\leq i\leq Q}, \mathsf{G}_{1,Q+1}, \mathsf{G}_2$ for the proof of Theorem 5.8.

G_0 is the real attack game and we have:

Lemma A.9 $\Pr[\mathsf{APR\text{-}CMA}^{\mathcal{A}}_{\mathsf{real}} \Rightarrow 1] = \Pr[\mathsf{G}_0^{\mathcal{A}} \Rightarrow 1]$.

In games $\mathsf{G}_{1,i}$, for the first $i-1$ queries to the EVAL oracle, $(u, \mathbf{u})$ is answered with uniformly random values and the rest are answered as in the real scheme. To interpolate between $\mathsf{G}_{1,i}$ and $\mathsf{G}_{1,i+1}$, we also define $\mathsf{G}_{1.1,i}$ to $\mathsf{G}_{1.3,i}$.

By the same arguments as in Appendix A.1, we have the following two lemmas:

Lemma A.10 $\Pr[\mathsf{G}_0^{\mathcal{A}} \Rightarrow 1] = \Pr[\mathsf{G}_{1,1}^{\mathcal{A}} \Rightarrow 1]$

Lemma A.11 *There exists an adversary $\mathcal{D}$ with $\mathbf{T}(\mathcal{D}) \approx \mathbf{T}(\mathcal{A})$ and $\mathbf{Adv}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{D}) \geq |\Pr[\mathsf{G}_{1.1,i}^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathsf{G}_{1,i}^{\mathcal{A}} \Rightarrow 1]|$.*

Lemma A.12 $|\Pr[\mathsf{G}_{1.2,i}^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathsf{G}_{1.1,i}^{\mathcal{A}} \Rightarrow 1]| \leq 1/q$.

Proof: Similar to Lemma A.4, let m be the i-th query to EVAL. As $\mathsf{m} \neq \mathsf{m}^*$, let i' be the smallest index such that $\mathsf{m}_{i'} \neq \mathsf{m}^*_{i'}$, where $\mathsf{m}_{i'}$ (resp. $\mathsf{m}^*_{i'}$) denotes the i'-th entry of m (resp. m^*). We apply an information-theoretical argument to show in $\mathsf{G}'_{1,i}$ the values u and $\mathbf{u}$ are uniformly random. For simplicity, we assume x'_0 and $\mathbf{x}_j$ ($j \notin \{0, i'\}$) are learned by $\mathcal{A}$. Similar to the proof of Lemma A.4, we assume $\mathcal{A}$ learns $\mathbf{B}^\top \mathbf{x}_0$ and $\mathbf{B}^\top \mathbf{x}_{i'}$. By the definition of APR-CMA security (Definition 5.7), m can not be a prefix of m^*. Thus, either ($i' \leq |\mathsf{m}^*|$ and $i' \leq |\mathsf{m}|$) (Case 1) or $i' \geq |\mathsf{m}^*| + 1$ and $\mathsf{m}^*_j = \mathsf{m}_j$ for all $j \leq |\mathsf{m}^*|$ (Case 2).

Case 1: From the execution of $\mathsf{G}_{1.1,i}$, $\mathcal{A}$ information-theoretically obtains the following equations in the unknown variables $\mathbf{x}_0, \mathbf{x}_{i'}$:

$$\begin{pmatrix} \mathbf{B}^\top \mathbf{x}_0 \\ \mathbf{B}^\top \mathbf{x}_{i'} \\ \mathbf{h}_0 \\ u - x'_0 \\ \mathbf{u} \end{pmatrix} = \begin{pmatrix} \mathbf{B}^\top & \mathbf{0} \\ \mathbf{0} & \mathbf{B}^\top \\ h \cdot \mathbf{I}_{k+1} & \mathsf{m}^*_{i'} h \cdot \mathbf{I}_{k+1} \\ \mathbf{t}^\top & \mathsf{m}_{i'} \mathbf{t}^\top \\ \mathbf{T}^\top & \mathsf{m}_{i'} \mathbf{T}^\top \end{pmatrix} \cdot \begin{pmatrix} \mathbf{x}_0 \\ \mathbf{x}_{i'} \end{pmatrix},$$

where $\mathbf{h}_0$ is from $\text{CHAL}(\mathsf{m}^*)$, u and $\mathbf{u}$ are from $\text{EVAL}(\mathsf{m})$, and $\mathbf{I}_{k+1}$ is the $(k+1) \times (k+1)$ identity matrix. We note that the terms $[d_{i'}]_2$ and $[\mathbf{D}_{i'}]_2$ from the c-th EVAL queries ($c \neq i$) only leak the information about $\mathbf{x}_{i'}$ on the span of $\mathbf{B}$. Since $(\mathbf{t}, \mathbf{T})$ is chosen uniformly from $\mathbb{Z}_q^{(k+1)\times(k+1)}$ in $\mathsf{G}_{1.1,i}$, $\mathbf{t}$ and $\mathbf{T}$ are not in the span of $\mathbf{B}$ and $(\mathbf{t}, \mathbf{T})$ has rank $k+1$ (except with probablity at most $1/q$), which implies $u - x'_0$ and $\mathbf{u}$ are independent from $\mathbf{B}^\top \mathbf{x}_0$ and $\mathbf{B}^\top \mathbf{x}_{i'}$ and $u - x'_0$ and $\mathbf{u}$ are independent from each other. By $\mathsf{m}_{i'} \neq \mathsf{m}^*_{i'}$, $u - x'_0$ and $\mathbf{u}$ are also independent of $\mathbf{h}_0$.

Case 2: Similarly, from the execution of $\mathsf{G}_{1.1,i}$, $\mathcal{A}$ information-theoretically obtains the following equations in the unknown variables $\mathbf{x}_0, \mathbf{x}_{i'}$:

$$\begin{pmatrix} \mathbf{B}^\top \mathbf{x}_0 \\ \mathbf{B}^\top \mathbf{x}_{i'} \\ \mathbf{h}_0 \\ u - x'_0 \\ \mathbf{u} \end{pmatrix} = \begin{pmatrix} \mathbf{B}^\top & \mathbf{0} \\ \mathbf{0} & \mathbf{B}^\top \\ h \cdot \mathbf{I}_{k+1} & \mathbf{0} \\ \mathbf{t}^\top & \mathsf{m}_{i'} \mathbf{t}^\top \\ \mathbf{T}^\top & \mathsf{m}_{i'} \mathbf{T}^\top \end{pmatrix} \cdot \begin{pmatrix} \mathbf{x}_0 \\ \mathbf{x}_{i'} \end{pmatrix}.$$

As in Case 1, $u - x'_0$ and $\mathbf{u}$ are linearly independent of $\mathbf{B}^\top \mathbf{x}_0$ and $\mathbf{B}^\top \mathbf{x}_i$. It is easy to see that $u - x'_0$ and $\mathbf{u}$ are linearly independent of $\mathbf{h}_0$. $u - x'_0$ and $\mathbf{u}$ are independent from each other, since $(\mathbf{t}, \mathbf{T})$ is a full rank matrix in $\mathbb{Z}_q^{(k+1)\times(k+1)}$

We conclude u and $\mathbf{u}$ are distributed uniformly at random in $\mathsf{G}_{1.1,i}$. ▮

We have the following two straightforward lemmas.

Lemma A.13 *There exists an adversary $\mathcal{D}$ with $\mathbf{T}(\mathcal{D}) \approx \mathbf{T}(\mathcal{A})$ and $\mathbf{Adv}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{D}) \geq |\Pr[\mathsf{G}_{1.3,i}^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathsf{G}_{1.2,i}^{\mathcal{A}} \Rightarrow 1]|$.*

Lemma A.14 $\Pr[\mathsf{G}_{1.3,i}^{\mathcal{A}} \Rightarrow 1] = \Pr[\mathsf{G}_{1,i+1}^{\mathcal{A}} \Rightarrow 1]$

Lemma A.15 $\Pr[\mathsf{G}_{2}^{\mathcal{A}} \Rightarrow 1] = \Pr[\mathsf{G}_{1,Q+1}^{\mathcal{A}} \Rightarrow 1]$.

Proof: Note that $\mathcal{A}$ can ask at most Q-many EVAL queries. In both $\mathsf{G}_{1,Q+1}$ and G_2, all answers of EVAL are uniformly random and independent of the secret keys $(x_0', \mathbf{x}_0, \dots, \mathbf{x}_L)$ where $L = \max\{|\mathsf{m}_1|, \dots, |\mathsf{m}_Q|\}$. Hence, the values $\mathbf{h}_0$ and h_1 from $\mathsf{G}_{1,Q+1}$ are uniform in the view of $\mathcal{A}$. ▮

We apply the above arguments in a reverse order, we have the following lemma.

Lemma A.16 *There exists an adversary $\mathcal{D}$ with $\mathbf{T}(\mathcal{D}) \approx \mathbf{T}(\mathcal{A})$ and* $|\Pr[\mathsf{APR\text{-}CMA}_{\mathsf{rand}}^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathsf{G}_2^{\mathcal{A}} \Rightarrow 1]| \leq Q(2\mathbf{Adv}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{D}) + 1/q)$.

B Security of the generic transformations

B.1 Security of HIBKEM transformation (Theorem 5.6)

The proof of Theorem 5.6 is similar to the one of Theorem 4.3. We define the sequence of games G_0-G_4 as in Figure 18. Let $\mathcal{A}$ be an adversary against the $\mathsf{IND\text{-}HID\text{-}CPA}$ security of $\mathsf{HIBKEM}[\mathsf{MAC}, \mathcal{D}_k]$. G_0 is the real attack game ($\mathsf{PR\text{-}HID\text{-}CPA}_{\mathsf{real}}$) and $\Pr[\mathsf{G}_0^{\mathcal{A}} \Rightarrow 1] = \Pr[\mathsf{PR\text{-}HID\text{-}CPA}_{\mathsf{real}}^{\mathcal{A}} \Rightarrow 1]$.

<u>INITIALIZE:</u> // Games G_0-G_2, $\boxed{\mathsf{G}_3\text{-}\mathsf{G}_4}$
$\mathcal{G} \xleftarrow{\$} \mathsf{GGen}(1^\lambda)$; $\mathbf{A} \xleftarrow{\$} \mathcal{D}_k$
$\mathsf{sk}_{\mathsf{MAC}} = (\mathbf{B}, \mathbf{x}_0, \dots, \mathbf{x}_\ell, x_0') \xleftarrow{\$} \mathsf{Gen}_{\mathsf{MAC}}(\mathcal{G})$
For $i = 0, \dots, \ell$:
  $\mathbf{Y}_i \xleftarrow{\$} \mathbb{Z}_q^{k \times n}$; $\mathbf{Z}_i = (\mathbf{Y}_i^\top \mid \mathbf{x}_i) \cdot \mathbf{A} \in \mathbb{Z}_q^{n \times k}$
  $\mathbf{d}_i = \mathbf{x}_i^\top \cdot \mathbf{B} \in \mathbb{Z}_q^{n'}$; $\mathbf{E}_i = \mathbf{Y}_i \cdot \mathbf{B} \in \mathbb{Z}_q^{k \times n'}$
  $\boxed{\mathbf{E}_i = (\overline{\mathbf{A}}^{-1})^\top (\mathbf{Z}_i^\top \mathbf{B} - \underline{\mathbf{A}}^\top \mathbf{d}_i)}$
$\mathbf{y}_0' \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{z}_0' = (\mathbf{y}_0'^\top \mid x_0') \cdot \mathbf{A} \in \mathbb{Z}_q^{1 \times k}$
$\mathsf{pk} := (\mathcal{G}, [\mathbf{A}]_1, ([\mathbf{Z}_i]_1)_{0 \le i \le \ell}, [\mathbf{z}_0']_1)$
$\mathsf{dk} := ([\mathbf{B}]_2, ([\mathbf{d}_i]_2, [\mathbf{E}_i]_2)_{0 \le i \le \ell})$
$\mathsf{sk} := (\mathsf{sk}_{\mathsf{MAC}}, (\mathbf{Y}_i)_{0 \le i \le \ell}, \mathbf{y}_0')$
Return $(\mathsf{pk}, \mathsf{dk})$

<u>USKGEN(id):</u> //Games G_0-G_2, $\boxed{\mathsf{G}_3\text{-}\mathsf{G}_4}$
$\mathcal{Q}_{\mathcal{ID}} = \mathcal{Q}_{\mathcal{ID}} \cup \{\mathsf{id}\}$
$([\mathbf{t}]_2, [u]_2) \xleftarrow{\$} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{id})$
$\mathbf{v} = \sum_{i=0}^{l(\mathsf{id})} f_i(\mathsf{id}) \mathbf{Y}_i \mathbf{t} + \mathbf{y}_0' \in \mathbb{Z}_q^k$
$\boxed{\mathbf{v}^\top = (\mathbf{t}^\top \sum f_i(\mathsf{id}) \mathbf{Z}_i + \mathbf{z}_0' - u \cdot \underline{\mathbf{A}}) \cdot \overline{\mathbf{A}}^{-1}}$
For $i = l(\mathsf{id}) + 1, \dots, \ell$:
  $d_i = \mathbf{x}_i^\top \mathbf{t} \in \mathbb{Z}_q$
  $\mathbf{e}_i = \mathbf{Y}_i \mathbf{t} \in \mathbb{Z}_q^k$;
  $\boxed{\mathbf{e}_i^\top = (\mathbf{t}^\top \mathbf{Z}_i - d_i \underline{\mathbf{A}}) \overline{\mathbf{A}}^{-1} \in \mathbb{Z}_q^{1 \times k}}$
$\mathsf{usk}[\mathsf{id}] := ([\mathbf{t}]_2, [u]_2, [\mathbf{v}]_2) \in \mathbb{G}_2^n \times \mathbb{G}_2^1 \times \mathbb{G}_2^k$
$\mathsf{udk}[\mathsf{id}] := ([d_i]_2, [\mathbf{e}_i]_2)_{l(\mathsf{id}) < i \le \ell} \in (\mathbb{G}_2^{1+k})^{(\ell - l(\mathsf{id}))}$
Return $(\mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}])$

<u>ENC(id*):</u> //Games G_0, $\boxed{\mathsf{G}_1\text{-}\mathsf{G}_2}$, G_2, G_3
$\mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^k$
$\mathbf{c}_0^* = \mathbf{A}\mathbf{r} \in \mathbb{Z}_q^{k+1}$
$\mathbf{c}_0^* \xleftarrow{\$} \mathbb{Z}_q^{k+1}$
$h \xleftarrow{\$} \mathbb{Z}_q$; $\overline{\mathbf{c}_0^*} \xleftarrow{\$} \mathbb{Z}_q^k$; $\underline{\mathbf{c}_0^*} := h + \underline{\mathbf{A}} \cdot \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}_0^*} \in \mathbb{Z}_q$
$\mathbf{c}_1^* = (\sum_{i=0}^{l(\mathsf{id}^*)} f_i(\mathsf{id}^*) \mathbf{Z}_i) \mathbf{r} \in \mathbb{Z}_q^n$
$\boxed{\mathbf{c}_1^* = \sum_{i=0}^{l(\mathsf{id}^*)} f_i(\mathsf{id}^*)(\mathbf{Y}_i^\top \mid \mathbf{x}_i) \mathbf{c}_0^* \in \mathbb{Z}_q^n}$
$\mathbf{c}_1^* = \sum_{i=0}^{\ell} f_i(\mathsf{id}^*)(\mathbf{Z}_i \cdot \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}_0^*} + \mathbf{x}_i \cdot h)$
$K^* = \mathbf{z}_0' \cdot \mathbf{r} \in \mathbb{Z}_q$.
$\boxed{K^* = (\mathbf{y}_0'^\top \mid x_0') \mathbf{c}_0^* \in \mathbb{Z}_q}$
$K^* = \mathbf{z}_0' \cdot \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}_0^*} + x_0' \cdot h$
Return $\mathsf{K}^* = [K^*]_T$ and $\mathsf{C}^* = ([\mathbf{c}_0^*]_1, [\mathbf{c}_1^*]_1)$

<u>ENC(id*):</u> //Game G_3, $\boxed{\mathsf{G}_4}$
$h \xleftarrow{\$} \mathbb{Z}_q$; $\overline{\mathbf{c}_0^*} \xleftarrow{\$} \mathbb{Z}_q^k$; $\underline{\mathbf{c}_0^*} := h + \underline{\mathbf{A}} \cdot \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}_0^*} \in \mathbb{Z}_q$
$\mathbf{c}_1^* = \sum_{i=0}^{\ell} f_i(\mathsf{id}^*)(\mathbf{Z}_i \cdot \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}_0^*} + \mathbf{x}_i \cdot h)$
$K^* = \mathbf{z}_0' \cdot \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}_0^*} + x_0' \cdot h$
$\boxed{K^* \xleftarrow{\$} \mathbb{Z}_q}$
Return $\mathsf{K}^* = [K^*]_T$ and $\mathsf{C}^* = ([\mathbf{c}_0^*]_1, [\mathbf{c}_1^*]_1)$

<u>FINALIZE(β):</u> //Games G_0-G_4
Return $(\mathsf{Prefix}(\mathsf{id}^*) \cap \mathcal{Q}_{\mathcal{ID}} = \emptyset) \wedge \beta$

Figure 18: Games G_0-G_4 for the proof of $\mathsf{IND\text{-}HID\text{-}CPA}$ security (Theorem 5.6).

By applying the same arguments as in Lemma 4.4 and 4.5, one can easily show the following two lemmas.

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

Lemma B.2 *There exists an adversary $\mathcal{B}_1$ with $\mathbf{T}(\mathcal{B}_1) \approx \mathbf{T}(\mathcal{A})$ and* $\mathbf{Adv}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}_1) \geq |\Pr[\mathsf{G}_2^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathsf{G}_1^{\mathcal{A}} \Rightarrow 1]|$.

<u>INITIALIZE:</u> $\mathbf{A} \xleftarrow{\$} \mathcal{D}_k$ $([\mathbf{B}]_2, ([\mathbf{x}_i^\top \mathbf{B}]_2)_{0\le i\le \ell}) \xleftarrow{\$} \textsc{Initialize}_{\mathsf{MAC}}$ For $i=0,\dots,\ell$: $\quad\mathbf{Z}_i \xleftarrow{\$} \mathbb{Z}_q^{n\times k}$; $\mathbf{d}_i := \mathbf{x}_i^\top \mathbf{B}$ $\quad\mathbf{E}_i = (\overline{\mathbf{A}}^{-1})^\top (\mathbf{Z}_i^\top \mathbf{B} - \underline{\mathbf{A}}^\top \mathbf{d}_i)$ $\mathbf{z}_0' \xleftarrow{\$} \mathbb{Z}_q^{1\times k}$ $\mathsf{pk} := (\mathcal{G}, [\mathbf{A}]_1, ([\mathbf{Z}_i]_1)_{0\le i\le\ell}, [\mathbf{z}_0']_1)$ $\mathsf{dk} := ([\mathbf{B}]_2, ([\mathbf{d}_i]_2, [\mathbf{E}_i]_2)_{0\le i\le\ell})$ Return $(\mathsf{pk}, \mathsf{dk})$ <u>ENC(id^*):</u> //only one query $([h]_1, [\mathbf{h}_0]_1, [h_1]_T) \xleftarrow{\$} \textsc{Chal}(\mathsf{id}^*)$ $\overline{\mathbf{c}}_0^* \xleftarrow{\$} \mathbb{Z}_q^k$; $\underline{\mathbf{c}}_0^* := h + \underline{\mathbf{A}}\cdot\overline{\mathbf{A}}^{-1}\overline{\mathbf{c}}_0^* \in \mathbb{Z}_q$ $\mathbf{c}_1^* = \sum_{i=0}^{l(\mathsf{id}^*)} f_i(\mathsf{id}^*)\mathbf{Z}_i \cdot \overline{\mathbf{A}}^{-1}\overline{\mathbf{c}}_0^* + \mathbf{h}_0$ $K^* = \mathbf{z}_0'\cdot \overline{\mathbf{A}}^{-1}\overline{\mathbf{c}}_0^* + h_1$ Return $\mathsf{K}^* = [K^*]_T$ and $\mathsf{C}^* = ([\mathbf{c}_0^*]_1, [\mathbf{c}_1^*]_1)$	<u>USKGEN(id):</u> $\mathcal{Q}_{\mathcal{ID}} = \mathcal{Q}_{\mathcal{ID}} \cup \{\mathsf{id}\}$ $([\mathbf{t}]_2,[u]_2,([d_i]_2)_{0\le i\le\ell}) \xleftarrow{\$} \textsc{Eval}(\mathsf{id})$ $\mathbf{v}^\top = (\mathbf{t}^\top \sum f_i(\mathsf{id})\mathbf{Z}_i + \mathbf{z}_0' - u\cdot\underline{\mathbf{A}})\cdot(\overline{\mathbf{A}})^{-1}$ For $i = l(\mathsf{id})+1,\dots,\ell$: $\quad\mathbf{e}_i^\top = (\mathbf{t}^\top \mathbf{Z}_i - d_i \underline{\mathbf{A}})\overline{\mathbf{A}}^{-1} \in \mathbb{Z}_q^{1\times k}$ $\mathsf{usk}[\mathsf{id}] := ([\mathbf{t}]_2,[u]_2,[\mathbf{v}]_2) \in \mathbb{G}_2^n \times \mathbb{G}_2^1 \times \mathbb{G}_2^k$ $\mathsf{udk}[\mathsf{id}] := ([d_i]_2, [\mathbf{e}_i]_2)_{l(\mathsf{id})<i\le\ell} \in (\mathbb{G}_2^{1+k})^{(\ell-l(\mathsf{id}))}$ Return $(\mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}])$ <u>FINALIZE(β):</u> Return $(\mathsf{Prefix}(\mathsf{id}^*) \cap \mathcal{Q}_{\mathcal{ID}} = \emptyset) \wedge \textsc{Finalize}_{\mathsf{MAC}}(\beta)$

Figure 19: Description of $\mathcal{B}_2$ (having access to the oracles $\textsc{Initialize}_{\mathsf{MAC}}, \textsc{Eval}, \textsc{Chal}, \textsc{Finalize}_{\mathsf{MAC}}$ of the $\mathsf{HPR\text{-}CMA}_{\mathsf{real}}/\mathsf{HPR\text{-}CMA}_{\mathsf{rand}}$ games of Figure 11) for the proof of Lemma B.4.

Lemma B.3 $\Pr[\mathsf{G}_3^{\mathcal{A}} \Rightarrow 1] = \Pr[\mathsf{G}_2^{\mathcal{A}} \Rightarrow 1]$.

Proof: Similar to the proof of Lemma 4.6, G_3 is simulated without using $\mathbf{y}_0'$ and $(\mathbf{Y}_i)_{0\le i\le\ell}$. By $\mathbf{Y}_i^\top = (\mathbf{Z}_i - \mathbf{x}_i\underline{\mathbf{A}})\overline{\mathbf{A}}^{-1}$, we have

$$\mathbf{E}_i = (\overline{\mathbf{A}}^{-1})^\top(\mathbf{Z}_i^\top\mathbf{B} - \underline{\mathbf{A}}^\top\mathbf{d}_i) = \underbrace{(\overline{\mathbf{A}}^{-1})^\top(\mathbf{Z}_i^\top - \underline{\mathbf{A}}^\top\mathbf{x}_i^\top)}_{\mathbf{Y}_i}\mathbf{B}$$

$$\mathbf{e}_i = (\overline{\mathbf{A}}^{-1})^\top \cdot (\mathbf{Z}_i^\top\mathbf{t} - \underline{\mathbf{A}}^\top \underbrace{\mathbf{x}_i^\top\mathbf{t}}_{d_i}) = \mathbf{Y}_i\mathbf{t}.$$

as in Game G_2. By the same argument as Lemma 4.6, we have $[\mathbf{v}]_2$, K^* and C^* are identical to G_2. ▌

Lemma B.4 *There exists an adversary $\mathcal{B}_2$ with $\mathbf{T}(\mathcal{B}_2) \approx \mathbf{T}(\mathcal{A})$ and $\mathsf{Adv}_{\mathsf{MAC}}^{\mathsf{hpr_0\text{-}cma}}(\mathcal{B}_2) \ge |\Pr[\mathsf{G}_4^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathsf{G}_3^{\mathcal{A}} \Rightarrow 1]|$*

Proof: In G_4, we answer the $\textsc{Enc}(\mathsf{id}^*)$ query by choosing random K^*. We construct algorithm $\mathcal{B}_2$ in Figure 19 to show the differences between G_4 and G_3 is bounded by the advantage of breaking $\mathsf{hpr_0\text{-}cma}$ security of MAC.

We note that, in games G_3 and G_4, the values $\mathbf{x}_i$ and x_i' are hidden until the call to $\textsc{Enc}(\mathsf{id}^*)$. In both games $\mathsf{HPR\text{-}CMA}_{\mathsf{real}}$ and $\mathsf{HPR_0\text{-}CMA}_{\mathsf{rand}}$, we have $h = \underline{\mathbf{c}}_0^* - \underline{\mathbf{A}}\overline{\mathbf{A}}^{-1}\overline{\mathbf{c}}_0^*$. Hence $\mathbf{h}_0 = \sum f_i(\mathsf{m}_i)\mathbf{x}_i \cdot (\underline{\mathbf{c}}_0^* - \underline{\mathbf{A}} \cdot \overline{\mathbf{A}}^{-1}\overline{\mathbf{c}}_0^*)$ which implies $\mathbf{c}_1^*$ is distributed identically in games G_3 and G_4. If h_1 is uniform (i.e., $\mathcal{B}_2$ is in Game $\mathsf{HPR_0\text{-}CMA}_{\mathsf{rand}}$) then the view of $\mathcal{A}$ is the same as in G_4. If h_1 is real (i.e., $\mathcal{B}_2$ is in Game $\mathsf{HPR\text{-}CMA}_{\mathsf{real}}$) then $K^* = \mathbf{z}_0' \cdot \overline{\mathbf{A}}^{-1}\overline{\mathbf{c}}_0^* + x_0' \cdot h$, which means the view of $\mathcal{A}$ is the same as in G_3. ▌

The proof follows by combining Lemmas B.1-B.4 and observing that $\mathsf{G}_4 = \mathsf{IND\text{-}HID\text{-}CPA}_{\mathsf{rand}}$.

B.2 Security of the Anonymous HIBKEM transformation (Theorem 5.9)

The proof of Theorem 5.9 is similar to the one of Theorem 5.6. We define the sequence of games G_0-G_4 in Figure 20. Let $\mathcal{A}$ be an adversary against the $\mathsf{PR\text{-}HID\text{-}CPA}$ security of $\mathsf{AHIBKEM}[\mathsf{MAC}, \mathcal{D}_k]$. G_0 is the real attack game ($\mathsf{PR\text{-}HID\text{-}CPA}_{\mathsf{real}}$) and $\Pr[\mathsf{G}_0^{\mathcal{A}} \Rightarrow 1] = \Pr[\mathsf{PR\text{-}HID\text{-}CPA}_{\mathsf{real}}^{\mathcal{A}} \Rightarrow 1]$.

<u>INITIALIZE:</u> // Games G_0-G_4
$\mathcal{G} \xleftarrow{\$} \mathsf{GGen}(1^\lambda)$; $\mathbf{A} \xleftarrow{\$} \mathcal{D}_k$
$\mathsf{sk}_{\mathsf{MAC}} = (\mathbf{B}, \mathbf{x}_0, \ldots, \mathbf{x}_\ell, x_0') \xleftarrow{\$} \mathsf{Gen}_{\mathsf{MAC}}(\mathcal{G})$
For $i = 0, \ldots, \ell$:
  $\mathbf{Y}_i \xleftarrow{\$} \mathbb{Z}_q^{k \times n}$; $\mathbf{Z}_i = (\mathbf{Y}_i^\top \mid \mathbf{x}_i) \cdot \mathbf{A} \in \mathbb{Z}_q^{n \times k}$
$\mathbf{y}_0' \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{z}_0' = (\mathbf{y}_0'^\top \mid x_0') \cdot \mathbf{A} \in \mathbb{Z}_q^{1 \times k}$
$\mathsf{pk} := (\mathcal{G}, [\mathbf{A}]_1, ([\mathbf{Z}_i]_1)_{0 \le i \le \ell}, [\mathbf{z}_0']_1)$
$\mathsf{sk} := (\mathsf{sk}_{\mathsf{MAC}}, (\mathbf{Y}_i)_{0 \le i \le \ell}, \mathbf{y}_0')$
Return pk

<u>USKGEN(id):</u> //Games G_0-G_2, $\boxed{\mathsf{G}_3\text{-}\mathsf{G}_4}$
$\mathcal{Q}_{\mathcal{ID}} = \mathcal{Q}_{\mathcal{ID}} \cup \{\mathsf{id}\}$
$([\mathbf{t}]_2, [u]_2) \xleftarrow{\$} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{id})$
$\mathbf{v} = \sum_{i=0}^{l(\mathsf{id})} f_i(\mathsf{id}) \mathbf{Y}_i \mathbf{t} + \mathbf{y}_0' \in \mathbb{Z}_q^k$
$\boxed{\mathbf{v}^\top = (\mathbf{t}^\top \sum f_i(\mathsf{id}) \mathbf{Z}_i + \mathbf{z}_0' - u \cdot \underline{\mathbf{A}}) \cdot \overline{\mathbf{A}}^{-1}}$
$\mathbf{S} \xleftarrow{\$} \mathbb{Z}_q^{n' \times \mu}$; $\mathbf{T} = \mathbf{B} \cdot \mathbf{S} \in \mathbb{Z}_q^{n \times \mu}$;
$\mathbf{u} = \sum_{i=0}^{l(\mathsf{id})} f_i(\mathsf{id}) \mathbf{x}_i^\top \mathbf{T} \in \mathbb{Z}_q^{1 \times \mu}$
$\mathbf{V} = \sum_{i=0}^{l(\mathsf{id})} f_i(\mathsf{id}) \mathbf{Y}_i \mathbf{T} \in \mathbb{Z}_q^{k \times \mu}$
$\boxed{\mathbf{V} = (\overline{\mathbf{A}}^{-1})^\top (\sum f_i(\mathsf{id}) \mathbf{Z}_i^\top \cdot \mathbf{T} - \underline{\mathbf{A}}^\top \cdot \mathbf{u})}$
For $i = l(\mathsf{id}) + 1, \ldots, \ell$:
  $d_i = \mathbf{x}_i^\top \mathbf{t} \in \mathbb{Z}_q$; $\mathbf{D}_i = \mathbf{x}_i^\top \mathbf{T} \in \mathbb{Z}_q^{1 \times \mu}$
  $\mathbf{e}_i = \mathbf{Y}_i \mathbf{t} \in \mathbb{Z}_q^k$; $\mathbf{E}_i = \mathbf{Y}_i \mathbf{T} \in \mathbb{Z}_q^{k \times \mu}$
  $\boxed{\mathbf{e}_i^\top = (\mathbf{t}^\top \mathbf{Z}_i - d_i \underline{\mathbf{A}}) \overline{\mathbf{A}}^{-1} \in \mathbb{Z}_q^{1 \times k}}$
  $\boxed{\mathbf{E}_i = (\overline{\mathbf{A}}^{-1})^\top (\mathbf{Z}_i^\top \mathbf{T} - \underline{\mathbf{A}}^\top \cdot \mathbf{D}_i) \in \mathbb{Z}_q^{k \times \mu}}$
$\mathsf{usk}[\mathsf{id}] := ([\mathbf{t}]_2, [u]_2, [\mathbf{v}]_2)$
$\mathsf{udk}[\mathsf{id}] := ([\mathbf{T}]_2, [\mathbf{u}]_2, [\mathbf{V}]_2, ([d_i]_2, [\mathbf{D}_i]_2, [\mathbf{e}_i]_2, [\mathbf{E}_i]_2)_{l(\mathsf{id}) < i \le \ell})$
Return $(\mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}])$

<u>ENC(id^*):</u> //Games G_0, $\boxed{\mathsf{G}_1\text{-}\mathsf{G}_2}$, G_2, G_3
$\mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^k$
$\mathbf{c}_0^* = \mathbf{A}\mathbf{r} \in \mathbb{Z}_q^{k+1}$
$\mathbf{c}_0^* \xleftarrow{\$} \mathbb{Z}_q^{k+1}$
$h \xleftarrow{\$} \mathbb{Z}_q$; $\overline{\mathbf{c}_0^*} \xleftarrow{\$} \mathbb{Z}_q^k$; $\underline{\mathbf{c}_0^*} := h + \underline{\mathbf{A}} \cdot \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}_0^*} \in \mathbb{Z}_q$
$\mathbf{c}_1^* = (\sum_{i=0}^{l(\mathsf{id}^*)} f_i(\mathsf{id}^*) \mathbf{Z}_i) \mathbf{r} \in \mathbb{Z}_q^n$
$\boxed{\mathbf{c}_1^* = \sum_{i=0}^{l(\mathsf{id}^*)} f_i(\mathsf{id}^*) (\mathbf{Y}_i^\top \mid \mathbf{x}_i) \mathbf{c}_0^* \in \mathbb{Z}_q^n}$
$\mathbf{c}_1^* = \sum_{i=0}^{\ell} f_i(\mathsf{id}^*) (\mathbf{Z}_i \cdot \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}_0^*} + \mathbf{x}_i \cdot h)$
$K^* = \mathbf{z}_0' \cdot \mathbf{r} \in \mathbb{Z}_q$.
$\boxed{K^* = (\mathbf{y}_0'^\top \mid x_0') \mathbf{c}_0^* \in \mathbb{Z}_q}$
$K^* = \mathbf{z}_0' \cdot \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}_0^*} + x_0' \cdot h$
Return $\mathsf{K}^* = [K^*]_T$ and $\mathsf{C}^* = ([\mathbf{c}_0^*]_1, [\mathbf{c}_1^*]_1)$.

<u>ENC(id^*):</u> //Game G_4
$\mathsf{K}^* \xleftarrow{\$} \mathbb{G}_T$; $\mathsf{C}^* \xleftarrow{\$} \mathbb{G}_1^{n+k+1}$
Return $\mathsf{K}^* = [K^*]_T$ and $\mathsf{C}^* = ([\mathbf{c}_0^*]_1, [\mathbf{c}_1^*]_1)$.

<u>FINALIZE(β):</u> //Games G_0-G_4
Return $(\mathsf{Prefix}(\mathsf{id}^*) \cap \mathcal{Q}_{\mathcal{ID}} = \emptyset) \wedge \beta$.

Figure 20: Games G_0-G_4 for the proof of PR-HID-CPA security (Theorem 5.9).

Analogously to Lemmas B.1 and B.2, we have

Lemma B.5 $\Pr[\mathsf{G}_1^{\mathcal{A}} \Rightarrow 1] = \Pr[\mathsf{G}_0^{\mathcal{A}} \Rightarrow 1]$.

Lemma B.6 *There exists an adversary $\mathcal{B}_1$ with $\mathbf{T}(\mathcal{B}_1) \approx \mathbf{T}(\mathcal{A})$ and $\mathbf{Adv}_{\mathcal{D}_k, \mathsf{GGen}}(\mathcal{B}_1) \ge |\Pr[\mathsf{G}_2^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathsf{G}_1^{\mathcal{A}} \Rightarrow 1]|$.*

Lemma B.7 $\Pr[\mathsf{G}_3^{\mathcal{A}} \Rightarrow 1] = \Pr[\mathsf{G}_2^{\mathcal{A}} \Rightarrow 1]$.

Proof: G_3 is defined without using $\mathbf{y}_0'$ and $(\mathbf{Y}_i)_{0 \le i \le \ell}$. By Lemma B.3, we have values $[\mathbf{v}]_2, [\mathbf{e}_i]_2, [\mathbf{E}_i]_2, \mathsf{K}^*$ and C^* are identical in both G_3 and G_2. By $\mathbf{Y}_i^\top = (\mathbf{Z}_i - \mathbf{x}_i \underline{\mathbf{A}}) \overline{\mathbf{A}}^{-1}$, we have

$$\mathbf{V} = \sum f_i(\mathsf{id}) (\overline{\mathbf{A}}^{-1})^\top (\mathbf{Z}_i^\top - \underline{\mathbf{A}}^\top \mathbf{x}_i^\top) \mathbf{T} = (\overline{\mathbf{A}}^{-1})^\top (\sum f_i(\mathsf{id}) \mathbf{Z}_i^\top \mathbf{T} - \underline{\mathbf{A}}^\top \underbrace{\sum f_i(\mathsf{id}) \mathbf{x}_i^\top \mathbf{T}}_{\mathbf{u}})$$

$$\mathbf{E}_i = (\overline{\mathbf{A}}^{-1})^\top (\mathbf{Z}_i^\top - \underline{\mathbf{A}}^\top \mathbf{x}_i^\top) \mathbf{T} = (\overline{\mathbf{A}}^{-1})^\top (\mathbf{Z}_i^\top \mathbf{T} - \underline{\mathbf{A}}^\top \underbrace{\mathbf{x}_i^\top \mathbf{T}}_{\mathbf{D}_i}).$$

Thus, G_3 is identical to G_2. ▌

Lemma B.8 *There exists an adversary $\mathcal{B}_2$ with $\mathbf{T}(\mathcal{B}_2) \approx \mathbf{T}(\mathcal{A})$ and $\mathsf{Adv}_{\mathsf{MAC}}^{\mathsf{apr\text{-}cma}}(\mathcal{B}_2) \ge |\Pr[\mathsf{G}_4^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathsf{G}_3^{\mathcal{A}} \Rightarrow 1]|$.*

$\underline{\textsc{Initialize}:}$	$\underline{\textsc{USKGen}(\mathsf{id}):}$
$\mathbf{A} \xleftarrow{\$} \mathcal{D}_k$; $\varepsilon \xleftarrow{\$} \textsc{Initialize}_{\mathsf{MAC}}$	$\mathcal{Q}_{\mathcal{ID}} = \mathcal{Q}_{\mathcal{ID}} \cup \{\mathsf{id}\}$
For $i = 0, \ldots, \ell$: $\mathbf{Z}_i \xleftarrow{\$} \mathbb{Z}_q^{n \times k}$	$([\mathbf{t}]_2, [u]_2, [\mathbf{T}]_2, [\mathbf{u}]_2, ([d_i]_2, [\mathbf{D}_i]_2)_{(\mathsf{m})<i\leq\ell}) \xleftarrow{\$} \textsc{Eval}(\mathsf{id})$
$\mathbf{z}'_0 \xleftarrow{\$} \mathbb{Z}_q^{1 \times k}$	$\mathbf{v}^\top = (\mathbf{t}^\top \sum f_i(\mathsf{id})\mathbf{Z}_i + \mathbf{z}'_0 - u \cdot \underline{\mathbf{A}}) \cdot (\overline{\mathbf{A}})^{-1}$
$\mathsf{pk} := (\mathcal{G}, [\mathbf{A}]_1, ([\mathbf{Z}_i]_1)_{0 \leq i \leq \ell}, [\mathbf{z}'_0]_1)$	$\mathbf{V} = (\overline{\mathbf{A}}^{-1})^\top (\sum f_i(\mathsf{id})\mathbf{Z}_i^\top \cdot \mathbf{T} - \underline{\mathbf{A}}^\top \cdot \mathbf{u})$
Return pk	For $i = l(\mathsf{id}) + 1, \ldots, \ell$:
	$\quad \mathbf{e}_i^\top = (\mathbf{t}^\top \mathbf{Z}_i - d_i \underline{\mathbf{A}})\overline{\mathbf{A}}^{-1} \in \mathbb{Z}_q^{1 \times k}$
$\underline{\textsc{Enc}(\mathsf{id}^*):}$ //only one query	$\quad \mathbf{E}_i = (\overline{\mathbf{A}}^{-1})^\top (\mathbf{Z}_i^\top \mathbf{T} - \underline{\mathbf{A}}^\top \cdot \mathbf{D}_i) \in \mathbb{Z}_q^{k \times \mu}$
$([h]_1, [\mathbf{h}_0]_1, [h_1]_T) \xleftarrow{\$} \textsc{Chal}(\mathsf{id}^*)$	$\mathsf{usk}[\mathsf{id}] := ([\mathbf{t}]_2, [u]_2, [\mathbf{v}]_2)$
$\overline{\mathbf{c}_0^*} \xleftarrow{\$} \mathbb{Z}_q^k$; $\underline{\mathbf{c}_0^*} := h + \underline{\mathbf{A}} \cdot \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}_0^*} \in \mathbb{Z}_q$	$\mathsf{udk}[\mathsf{id}] := ([\mathbf{T}]_2, [\mathbf{u}]_2, [\mathbf{V}]_2, ([d_i]_2, [\mathbf{D}_2], [\mathbf{e}_i]_2, [\mathbf{E}_i]_2)_{l(\mathsf{id})<i\leq\ell})$
$\mathbf{c}_1^* = \sum_{i=0}^{l(\mathsf{id}^*)} f_i(\mathsf{id}^*)\mathbf{Z}_i \cdot \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}_0^*} + \mathbf{h}_0$	Return $(\mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}])$.
$K^* = \mathbf{z}'_0 \cdot \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}_0^*} + h_1$	$\underline{\textsc{Finalize}(\beta):}$
Return $\mathsf{K}^* = [K^*]_T$ and $\mathsf{C}^* = ([\mathbf{c}_0^*]_1, [\mathbf{c}_1^*]_1)$.	Return $(\mathsf{Prefix}(\mathsf{id}^*) \cap \mathcal{Q}_{\mathcal{ID}} = \emptyset) \wedge \textsc{Finalize}_{\mathsf{MAC}}(\beta)$.

Figure 21: Description of $\mathcal{B}_2$ (having access to the oracles $\textsc{Initialize}_{\mathsf{MAC}}, \textsc{Eval}, \textsc{Chal}, \textsc{Finalize}_{\mathsf{MAC}}$ of the $\mathsf{APR\text{-}CMA}_{\mathsf{real}}/\mathsf{APR\text{-}CMA}_{\mathsf{rand}}$ games of Figure 14) for the proof of Lemma B.8.

Proof: In G_4, we answer the $\textsc{Enc}(\mathsf{id}^*)$ query by choosing random K^* and C^*. We construct algorithm $\mathcal{B}_2$ in Figure 21 to show the differences between G_4 and G_3 is bounded by the advantage of breaking APR-CMA security of MAC.

We note that, in both G_3 and G_4, the values $\mathbf{x}_i$ and x'_0 are hidden until the call to $\textsc{Enc}(\mathsf{id}^*)$. It is easy to see $\mathbf{c}_0^*$ is uniform, since h and $\bar{\mathbf{c}}_0^*$ are chosen uniformly at random. If $(\mathbf{h}_0, h_1)$ is uniform (i.e. $\mathcal{B}_2$ is in Game $\mathsf{APR\text{-}CMA}_{\mathsf{rand}}$) then the view of $\mathcal{A}$ is the same as in G_4. If $(\mathbf{h}_0, h_1)$ is real (i.e. $\mathcal{B}_2$ is in Game $\mathsf{APR\text{-}CMA}_{\mathsf{real}}$) then the view of $\mathcal{A}$ is the same as in G_3. ▮

The proof follows by combining Lemmas B.5-B.8 and observing that $\mathsf{G}_4 = \mathsf{PR\text{-}HID\text{-}CPA}_{\mathsf{rand}}$.

C Identity-based Hash Proof System

In this section, we will show that our IBE construction from Section 4 gives a secure identity-based hash proof system (ID-HPS) [1], which implies IND-CCA secure [20] and leakage-resilent [1] IBE. Moreover, one of our constructions is the first tightly secure ID-HPS without a "q-type" assumption in prime-order groups.

C.1 Definitions

We recall syntax and security of ID-HPS from [1].

Definition C.1 (Identity-based Hash Proof System) *An identity-based hash proof system (ID-HPS) consists of five PPT algorithms* $\mathsf{IDHPS} = (\mathsf{Setup}, \mathsf{USKGen}, \mathsf{Encap}, \mathsf{Encap}^*, \mathsf{Decap})$ *with the following properties.*

- *The probabilistic key generation algorithm* $\mathsf{Setup}(\mathsf{par})$ *returns the (master) public/secret key* $(\mathsf{pk}, \mathsf{sk})$. *We assume that* pk *implicitly defines an identity space* $\mathcal{ID}$*, an encapsulated-key set* $\mathcal{K}$.
- *The probabilistic user secret key generation algorithm* $\mathsf{USKGen}(\mathsf{sk}, \mathsf{id})$ *returns the secret key* $\mathsf{usk}[\mathsf{id}]$ *for an identity* $\mathsf{id} \in \mathcal{ID}$.
- *The probabilistic* valid *encapsulation algorithm* $\mathsf{Encap}(\mathsf{pk}, \mathsf{id})$ *returns a pair* (c, K) *where c is a valid ciphertext, and* $\mathsf{K} \in \mathcal{K}$ *is the encapsulated-key with respect to identity* id.
- *The probabilistic* invalid *encapsulation algorithm* $\mathsf{Encap}^*(\mathsf{pk}, \mathsf{id})$ *samples an invalid ciphertext c.*
- *The deterministic decapsulation algorithm* $\mathsf{Decap}(\mathsf{usk}[\mathsf{id}], c)$ *returns a decapsulated key* K.

For perfect correctness we require that for all $\lambda \in \mathbb{N}$*, all pairs* $(\mathsf{pk}, \mathsf{sk})$ *generated by* $\mathsf{Setup}(1^\lambda)$*, all identities* $\mathsf{id} \in \mathcal{ID}$*, all* $\mathsf{usk}[\mathsf{id}]$ *generated by* $\mathsf{USKGen}(\mathsf{sk}, \mathsf{id})$ *and all* (c, K) *output by* $\mathsf{Encap}(\mathsf{pk}, \mathsf{id})$*:*

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

The security requirements for an ID-HPS are valid/invalid ciphertext indistinguishability ($\mathsf{VI\text{-}IND}$) and smoothness. $\mathsf{VI\text{-}IND}$ security is defined via the games $\mathsf{VI\text{-}IND}_{\mathsf{real}}$ and $\mathsf{VI\text{-}IND}_{\mathsf{rand}}$ in Figure 22. Note that $\mathsf{VI\text{-}IND}$ security game, the adversary is allowed to ask for $\mathsf{usk}[\mathsf{id}^*]$ (where id^* is the challenge identity) and that USKGEN(id) returns the same answer when queried twice on the same identity.

Definition C.2 ($\mathsf{VI\text{-}IND}$ Security) *An identity-based hash proof system* IDHPS *is* $\mathsf{VI\text{-}IND}$*-secure if for all PPT* $\mathcal{A}$, $\mathsf{Adv}^{\mathsf{vi\text{-}ind}}_{\mathsf{IDHPS}}(\mathcal{A}) := |\Pr[\mathsf{VI\text{-}IND}^{\mathcal{A}}_{\mathsf{real}} \Rightarrow 1] - \Pr[\mathsf{VI\text{-}IND}^{\mathcal{A}}_{\mathsf{rand}} \Rightarrow 1]|$ *is negligible.*

INITIALIZE:	USKGEN(id):
$(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\$} \mathsf{Setup}(\mathsf{par})$	If $\mathsf{usk}[\mathsf{id}] = \perp$, then
Return pk	$\quad \mathsf{usk}[\mathsf{id}] \xleftarrow{\$} \mathsf{USKGen}(\mathsf{sk}, \mathsf{id})$
	$\quad \mathcal{Q}_{\mathcal{ID}} := (\mathsf{id}, \mathsf{usk}[\mathsf{id}]) \cup \mathcal{Q}_{\mathcal{ID}}$
ENC(id^*): //one query	Return $\mathsf{usk}[\mathsf{id}]$
$(\mathsf{C}^*, \mathsf{K}^*) \xleftarrow{\$} \mathsf{Encap}(\mathsf{pk}, \mathsf{id}^*)$	
$\boxed{\mathsf{C}^* \xleftarrow{\$} \mathsf{Encap}^*(\mathsf{pk}, \mathsf{id}^*)}$	FINALIZE(β'):
Return C^*	Return β'

Figure 22: Games $\mathsf{VI\text{-}IND}_{\mathsf{real}}$ and $\boxed{\mathsf{VI\text{-}IND}_{\mathsf{rand}}}$ for defining valid/invalid ciphertext indistinguishability. We note that in game $\mathsf{VI\text{-}IND}_{\mathsf{rand}}$ the adversary is allowed to query USKGEN with the challenge id^*.

Smoothness is a statistical property saying that the decapsulated key K for an *invalid* ciphertext is distributed statistically close to the uniform distribution.

Definition C.3 (Statistical Distance) *The statistical distance between two random variables* X *and* Y *over a finite domain* Ω *is defined as:*

$$\mathbf{SD}(X, Y) := \frac{1}{2} \sum_{w \in \Omega} |\Pr[X = w] - \Pr[Y = w]|.$$

Definition C.4 (Smooth ID-HPS) *An identity-based hash proof system* IDHPS *is* smooth *if for any fixed* $(\mathsf{pk}, \mathsf{sk})$ *produced by* $\mathsf{Setup}(\mathsf{par})$*, any* $\mathsf{id} \in \mathcal{ID}$*,*

$$\mathbf{SD}((\mathsf{C}, \mathsf{K}), (\mathsf{C}, \mathsf{K}')) \leq \mathit{negl}(\lambda),$$

where $\mathsf{C} \xleftarrow{\$} \mathsf{Encap}^*(\mathsf{id})$*,* $\mathsf{K} \leftarrow \mathsf{Decap}(\mathsf{C}, \mathsf{usk}[\mathsf{id}])$*,* $\mathsf{K}' \xleftarrow{\$} \mathcal{K}$ *and* $\mathsf{usk}[\mathsf{id}] \xleftarrow{\$} \mathsf{USKGen}(\mathsf{sk}, \mathsf{id})$.

C.2 Construction

Let $\mathcal{D}_k$ be a matrix distribution that outputs matrices $\mathbf{A} \in \mathbb{Z}_q^{(k+1)\times k}$. Let MAC be an affine MAC over $\mathbb{Z}_q^n$ with message space $\mathcal{ID}$. In Figure 23, we describe the transformation $\mathsf{IDHPS}[\mathsf{MAC}, \mathcal{D}_k]$. We note that $\mathsf{Setup}, \mathsf{USKGen}, \mathsf{Encap}$ and Decap are the same as in $\mathsf{IBKEM}[\mathsf{MAC}, \mathcal{D}_k]$ from Section 4 and Encap^* returns a random ciphertext C from the ciphertext space $\mathcal{C} = \mathbb{G}_1^{n+k+1}$. Correctness of $\mathsf{IDHPS}[\mathsf{MAC}, \mathcal{D}_k]$ follows from the correctness of $\mathsf{IBE}[\mathsf{MAC}, \mathcal{D}_k]$.

C.3 Security

We show that our ID-HPS is both smooth and $\mathsf{VI\text{-}IND}$ secure.

For the proof of $\mathsf{VI\text{-}IND}$ security, we require a security notion for the affine MAC that is slightly stronger than $\mathsf{PR\text{-}CMA}$ security in the sense that we allow the adversary to query EVAL with the challenge message m^* in order to fit the definition of $\mathsf{VI\text{-}IND}$ security. We call it *strong pseudorandomness against chosen-message attacks* ($\mathsf{SPR\text{-}CMA}$) defined via the security games in Figure 24.

Definition C.5 *An affine* MAC *over* $\mathbb{Z}_q^n$ *is* $\mathsf{SPR\text{-}CMA}$*-secure if for all PPT* $\mathcal{A}$, $\mathsf{Adv}^{\mathsf{spr\text{-}cma}}_{\mathsf{MAC}}(\mathcal{A}) := \Pr[\mathsf{SPR\text{-}CMA}^{\mathcal{A}}_{\mathsf{real}} \Rightarrow 1] - \Pr[\mathsf{SPR\text{-}CMA}^{\mathcal{A}}_{\mathsf{rand}} \Rightarrow 1]$ *is negligible, where the experiments are defined in Figure 24.*

Setup(par):	Encap(pk, id):
$\mathbf{A} \stackrel{\$}{\leftarrow} \mathcal{D}_k$	$\mathbf{r} \stackrel{\$}{\leftarrow} \mathbb{Z}_q^k$
$\mathsf{sk}_{\mathsf{MAC}} = (\mathbf{B}, \mathbf{x}_0, \ldots, \mathbf{x}_\ell, x'_0, \ldots, x'_{\ell'}) \stackrel{\$}{\leftarrow} \mathsf{Gen}_{\mathsf{MAC}}(\mathsf{par})$	$\mathbf{c}_0 = \mathbf{A}\mathbf{r} \in \mathbb{Z}_q^{k+1}$
For $i = 0, \ldots, \ell : \mathbf{Y}_i \stackrel{\$}{\leftarrow} \mathbb{Z}_q^{k \times n}; \mathbf{Z}_i = (\mathbf{Y}_i^\top \mid \mathbf{x}_i) \cdot \mathbf{A} \in \mathbb{Z}_q^{n \times k}$	$\mathbf{c}_1 = (\sum_{i=0}^{\ell} f_i(\mathsf{id})\mathbf{Z}_i) \cdot \mathbf{r} \in \mathbb{Z}_q^n$
For $i = 0, \ldots, \ell' : \mathbf{y}'_i \stackrel{\$}{\leftarrow} \mathbb{Z}_q^k; \mathbf{z}'_i = (\mathbf{y}'^\top_i \mid x'_i) \cdot \mathbf{A} \in \mathbb{Z}_q^{1 \times k}$	$K = (\sum_{i=0}^{\ell'} f'_i(\mathsf{id})\mathbf{z}'_i) \cdot \mathbf{r} \in \mathbb{Z}_q$.
$\mathsf{pk} := (\mathcal{G}, [\mathbf{A}]_1, ([\mathbf{Z}_i]_1)_{0 \le i \le \ell}, ([\mathbf{z}'_i]_1)_{0 \le i \le \ell'})$	Return $\mathsf{K} = [K]_T$ and $\mathsf{C} = ([\mathbf{c}_0]_1, [\mathbf{c}_1]_1) \in \mathbb{G}_1^{n+k+1}$
$\mathsf{sk} := (\mathsf{sk}_{\mathsf{MAC}}, (\mathbf{Y}_i)_{0 \le i \le \ell}, (\mathbf{y}'_i)_{0 \le i \le \ell'})$	
Return $(\mathsf{pk}, \mathsf{sk})$	$\mathsf{Encap}^*(\mathsf{pk}, \mathsf{id})$:
	$(\mathbf{c}_0, \mathbf{c}_1) \stackrel{\$}{\leftarrow} \mathbb{Z}_q^{n+k+1}$
USKGen(sk, id):	Return $\mathsf{C} = ([\mathbf{c}_0]_1, [\mathbf{c}_1]_1) \in \mathbb{G}_1^{n+k+1}$
$([\mathbf{t}]_2, [u]_2) \stackrel{\$}{\leftarrow} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{id})$	
$\mathbf{v} = \sum_{i=0}^{\ell} f_i(\mathsf{id})\mathbf{Y}_i\mathbf{t} + \sum_{i=0}^{\ell'} f'_i(\mathsf{id})\mathbf{y}'_i \in \mathbb{Z}_q^k$	Decap(usk[id], C):
Return $\mathsf{usk}[\mathsf{id}] := ([\mathbf{t}]_2, [u]_2, [\mathbf{v}]_2) \in \mathbb{G}_2^{n+1+k}$	Parse $\mathsf{usk}[\mathsf{id}] = ([\mathbf{t}]_2, [u]_2, [\mathbf{v}]_2)$
	Parse $\mathsf{C} = ([\mathbf{c}_0]_1, [\mathbf{c}_1]_1)$
	$\mathsf{K} = e([\mathbf{c}_0]_1, \begin{bmatrix} \mathbf{v} \\ u \end{bmatrix}_2) - e([\mathbf{c}_1]_1, [\mathbf{t}]_2)$
	Return $\mathsf{K} \in \mathbb{G}_T$

Figure 23: Definition of the ID-based HPS $\mathsf{IDHPS}[\mathsf{MAC}, \mathcal{D}_k]$.

INITIALIZE:	EVAL(m):
$\mathsf{sk}_{\mathsf{MAC}} \stackrel{\$}{\leftarrow} \mathsf{Gen}_{\mathsf{MAC}}(\mathsf{par})$	If $(\mathbf{t}[\mathsf{m}], u[\mathsf{m}]) = (\perp, \perp)$ then
Return ε	$([\mathbf{t}[\mathsf{m}]]_2, [u[\mathsf{m}]]_2) \stackrel{\$}{\leftarrow} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m})$
	$\boxed{\mathbf{t}[\mathsf{m}] \stackrel{\$}{\leftarrow} \mathbb{Z}_q^n; \mathbf{h}_0[\mathsf{m}] \stackrel{\$}{\leftarrow} \mathbb{Z}_q^n; h_1[\mathsf{m}] \stackrel{\$}{\leftarrow} \mathbb{Z}_q}$
CHAL(m^*): //one query	$\boxed{u[\mathsf{m}] = \mathbf{h}_0[\mathsf{m}] \cdot \mathbf{t}[\mathsf{m}] + h_1[\mathsf{m}]}$
$h \stackrel{\$}{\leftarrow} \mathbb{Z}_q$; $\mathbf{h}_0[\mathsf{m}^*] = \sum f_i(\mathsf{m}^*)\mathbf{x}_i \in \mathbb{Z}_q^n$	Return $([\mathbf{t}[\mathsf{m}]]_2, [u[\mathsf{m}]]_2)$
$\boxed{([\mathbf{t}]_2, [u]_2) \stackrel{\$}{\leftarrow} \text{EVAL}(\mathsf{m}^*)}$	
Return $([h]_1, [\mathbf{h}_0[\mathsf{m}^*] \cdot h]_1)$	FINALIZE($d \in \{0, 1\}$):
	Return d

Figure 24: Games $\mathsf{SPR\text{-}CMA}_{\mathsf{real}}$ and $\boxed{\mathsf{SPR\text{-}CMA}_{\mathsf{rand}}}$ for defining SPR-CMA security.

We note that both $\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k]$ and $\mathsf{MAC}_{\mathsf{HPS}}[\mathcal{D}_k]$ are SPR-CMA secure. The security proof from Section 3 can be easily adapted to show both schemes are SPR-CMA secure. Here we just outline the ideas. For $\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k]$, we first use the Q-fold $\mathcal{D}_k$-MDDH assumption to make the answers all EVAL queries random; next, we store a list of $(\mathbf{h}_0[\cdot], h_1[\cdot])$ values to make the output of CHAL(m^*) random and consistent with EVAL(m^*). One can also adapt the proof of $\mathsf{MAC}_{\mathsf{HPS}}[\mathcal{D}_k]$ in a similar way.

The following theorem shows VI-IND security of $\mathsf{IDHPS}[\mathsf{MAC}, \mathcal{D}_k]$.

Theorem C.6 *Under the $\mathcal{D}_k$-MDDH assumption relative to GGen in $\mathbb{G}_1$ and SPR-CMA security of MAC, $\mathsf{IDSPHF}[\mathsf{MAC}, \mathcal{D}_k]$ is a VI-IND secure ID-SPHF. Particularly, for all adversaries $\mathcal{A}$ there exist adversaries $\mathcal{B}_1$ and $\mathcal{B}_2$ with $\mathbf{T}(\mathcal{B}_1) \approx \mathbf{T}(\mathcal{A}) \approx \mathbf{T}(\mathcal{B}_2)$ and $\mathsf{Adv}^{\mathsf{vi\text{-}ind}}_{\mathsf{IDHPS}[\mathsf{MAC}, \mathcal{D}_k]}(\mathcal{A}) \le \mathbf{Adv}_{\mathcal{D}_k, \mathsf{GGen}}(\mathcal{B}_1) + \mathsf{Adv}^{\mathsf{spr\text{-}cma}}_{\mathsf{MAC}}(\mathcal{B}_2)$.*

Proof: The proof is similar to the one of Theorem 4.3 except that we need to simulate the user secret key for the challenge identity id^*. The games are defined as in Figure 25.

The following three lemmas and their proofs are exactly the same as Lemmas 4.4 to 4.6.

Lemma C.7 $\Pr[\mathsf{VI\text{-}IND}^{\mathcal{A}}_{\mathsf{real}} \Rightarrow 1] = \Pr[\mathsf{G}_1^{\mathcal{A}} \Rightarrow 1] = \Pr[\mathsf{G}_0^{\mathcal{A}} \Rightarrow 1]$.

Lemma C.8 *There exists an adversary $\mathcal{B}_1$ with $\mathbf{T}(\mathcal{B}_1) \approx \mathbf{T}(\mathcal{A})$ and $\mathbf{Adv}_{\mathcal{D}_k, \mathsf{GGen}}(\mathcal{B}_1) \ge |\Pr[\mathsf{G}_2^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathsf{G}_1^{\mathcal{A}} \Rightarrow 1]|$.*

$\underline{\text{INITIALIZE:}}$ // Games G_0-G_4

$\mathcal{G} \xleftarrow{\$} \mathsf{GGen}(1^\lambda)$; $\mathbf{A} \xleftarrow{\$} \mathcal{D}_k$

$\mathsf{sk}_{\mathsf{MAC}} = (\mathbf{B}, \mathbf{x}_0, \ldots, \mathbf{x}_\ell, x'_0, \ldots, x'_{\ell'}) \xleftarrow{\$} \mathsf{Gen}_{\mathsf{MAC}}(\mathcal{G})$

For $i = 0, \ldots, \ell : \mathbf{Y}_i \xleftarrow{\$} \mathbb{Z}_q^{k \times n}; \mathbf{Z}_i = (\mathbf{Y}_i^\top \mid \mathbf{x}_i) \cdot \mathbf{A} \in \mathbb{Z}_q^{n \times k}$

For $i = 0, \ldots, \ell' : \mathbf{y}'_i \xleftarrow{\$} \mathbb{Z}_q^{k}; \mathbf{z}'_i = ({\mathbf{y}'_i}^\top \mid x'_i) \cdot \mathbf{A} \in \mathbb{Z}_q^{1 \times k}$

$\mathsf{pk} := (\mathcal{G}, [\mathbf{A}]_1, ([\mathbf{Z}_i]_1)_{0 \le i \le \ell}, ([\mathbf{z}'_i]_1)_{0 \le i \le \ell'})$

$\mathsf{sk} := (\mathsf{sk}_{\mathsf{MAC}}, (\mathbf{Y}_i)_{0 \le i \le \ell}, (\mathbf{y}'_i)_{0 \le i \le \ell'})$

Return pk

$\underline{\text{USKGEN}(\mathsf{id}):}$ //Games G_0-G_2, $\boxed{\mathsf{G}_3\text{-}\mathsf{G}_4}$, G_4

If $\mathsf{usk}[\mathsf{id}] = \perp$ then

$([\mathbf{t}]_2, [u]_2) \xleftarrow{\$} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{id})$

$\mathbf{t} \xleftarrow{\$} \mathbb{Z}_q^n; \mathbf{h}_0[\mathsf{id}] \xleftarrow{\$} \mathbb{Z}_q^n; h_1[\mathsf{id}] \xleftarrow{\$} \mathbb{Z}_q$

$u = \mathbf{h}_0[\mathsf{id}]\mathbf{t} + h_1[\mathsf{id}]$

$\mathbf{v} = \sum_{i=0}^{\ell} f_i(\mathsf{id})\mathbf{Y}_i\mathbf{t} + \sum_{i=0}^{\ell'} f'_i(\mathsf{id})\mathbf{y}'_i \in \mathbb{Z}_q^k$

$\boxed{\mathbf{v}^\top = (\mathbf{t}^\top \sum f_i(\mathsf{id})\mathbf{Z}_i + \sum f'_i(\mathsf{id})\mathbf{z}'_i - u \cdot \underline{\mathbf{A}}) \cdot \overline{\mathbf{A}}^{-1}}$

$\mathsf{usk}[\mathsf{id}] := ([\mathbf{t}]_2, [u]_2, [\mathbf{v}]_2) \in \mathbb{G}_2^n \times \mathbb{G}_2^1 \times \mathbb{G}_2^k$

Return $\mathsf{usk}[\mathsf{id}]$

$\underline{\text{ENC}(\mathsf{id}^*):}$ //Games G_0, $\boxed{\mathsf{G}_1\text{-}\mathsf{G}_2}$, G_2, G_3

$\mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^k$

$\mathbf{c}_0^* = \mathbf{A}\mathbf{r} \in \mathbb{Z}_q^{k+1}$; $\mathbf{c}_0^* \xleftarrow{\$} \mathbb{Z}_q^{k+1}$

$h \xleftarrow{\$} \mathbb{Z}_q, \overline{\mathbf{c}_0^*} \xleftarrow{\$} \mathbb{Z}_q^k$; $\underline{\mathbf{c}_0^*} := h + \underline{\mathbf{A}} \cdot \overline{\mathbf{A}}^{-1}\overline{\mathbf{c}_0^*} \in \mathbb{Z}_q$

$\mathbf{c}_1^* = (\sum_{i=0}^{\ell} f_i(\mathsf{id}^*)\mathbf{Z}_i)\mathbf{r} \in \mathbb{Z}_q^n$

$\boxed{\mathbf{c}_1^* = \sum_{i=0}^{\ell} f_i(\mathsf{id}^*)(\mathbf{Y}_i^\top \mid \mathbf{x}_i)\mathbf{c}_0^* \in \mathbb{Z}_q^n}$

$\mathbf{c}_1^* = \sum_{i=0}^{\ell} f_i(\mathsf{id}^*)(\mathbf{Z}_i \cdot \overline{\mathbf{A}}^{-1}\overline{\mathbf{c}_0^*} + \mathbf{x}_i \cdot h)$

Return $\mathsf{C}^* = ([\mathbf{c}_0^*]_1, [\mathbf{c}_1^*]_1)$

$\underline{\text{ENC}(\mathsf{id}^*):}$ //Game G_4

Call $\mathsf{usk}[\mathsf{id}^*] \xleftarrow{\$} \text{USKGEN}(\mathsf{id}^*)$

$h \xleftarrow{\$} \mathbb{Z}_q, \overline{\mathbf{c}_0^*} \xleftarrow{\$} \mathbb{Z}_q^k$; $\underline{\mathbf{c}_0^*} := h + \underline{\mathbf{A}} \cdot \overline{\mathbf{A}}^{-1}\overline{\mathbf{c}_0^*} \in \mathbb{Z}_q$

$\mathbf{c}_1^* = \sum_{i=0}^{\ell} f_i(\mathsf{id}^*)(\mathbf{Z}_i \cdot \overline{\mathbf{A}}^{-1}\overline{\mathbf{c}_0^*}) + \mathbf{h}_0[\mathsf{id}^*] \cdot h$

Return $\mathsf{C}^* := ([\mathbf{c}_0^*]_1, [\mathbf{c}_1^*]_1)$

$\underline{\text{FINALIZE}(\beta'):}$ //Game G_1-G_4

Return β'

Figure 25: Games G_0-G_4 for the proof of the VI-IND security.

Lemma C.9 $\Pr[\mathsf{G}_3^{\mathcal{A}} \Rightarrow 1] = \Pr[\mathsf{G}_2^{\mathcal{A}} \Rightarrow 1]$.

Lemma C.10 *There exists an adversary* $\mathcal{B}_2$ *with* $\mathbf{T}(\mathcal{B}_2) \approx \mathbf{T}(\mathcal{A})$ *and* $\mathsf{Adv}_{\mathsf{MAC}}^{\mathsf{spr\text{-}cma}}(\mathcal{B}_2) \ge |\Pr[\mathsf{G}_4^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathsf{G}_3^{\mathcal{A}} \Rightarrow 1]|$.

Proof: We construct an adversary $\mathcal{B}_2$ in Figure 26 to show that the difference between G_4 and G_3 is bounded by the advantage of breaking SPR-CMA security of MAC.

By the definition of SPR-CMA, if $\mathcal{B}_2$ is in Game $\mathsf{SPR\text{-}CMA}_{\mathsf{rand}}$ then the view of $\mathcal{A}$ is the same as in G_4; and if $\mathcal{B}_2$ is in Game $\mathsf{SPR\text{-}CMA}_{\mathsf{real}}$ then the view of $\mathcal{A}$ is the same as in G_3. ▌

We observe that in Game G_4 $\mathbf{c}_1^*$ is masked by the value $\mathbf{h}_0[\mathsf{id}^*]$, which is uniformly random. The reason is that $\mathbf{h}_0[\mathsf{id}^*]$ is hidden from $\text{USKGEN}(\mathsf{id}^*)$ query, since it is masked by a random $h_1[\mathsf{id}^*]$. Thus, $\mathsf{G}_4 = \mathsf{VI\text{-}IND}_{\mathsf{rand}}$. ▌

Theorem C.11 $\mathsf{IDHPS}[\mathsf{MAC}, \mathcal{D}_k]$ *is smooth.*

Proof: We show that for almost all $(\mathbf{c}_0, \mathbf{c}_1) \in \mathbb{Z}_q^{n+k+1}$, $K = \mathbf{c}_0^\top \begin{pmatrix} \mathbf{v} \\ u \end{pmatrix} - \mathbf{c}_1^\top \mathbf{t}$ is uniformly random, where $([\mathbf{t}]_2, [u]_2, [\mathbf{v}]_2) \xleftarrow{\$} \mathsf{USKGen}(\mathsf{id})$. Similar to game G_3 of VI-IND security proof, one can rewrite:

$$
\begin{aligned}
K &= \mathbf{c}_0^\top \begin{pmatrix} \mathbf{v} \\ u \end{pmatrix} - \mathbf{c}_1^\top \mathbf{t} \\
&= \mathbf{c}_0^\top \begin{pmatrix} ((\mathbf{t}^\top \sum f_i(\mathsf{id})\mathbf{Z}_i + \sum f'_i(\mathsf{id})\mathbf{z}'_i - u \cdot \underline{\mathbf{A}}) \cdot \overline{\mathbf{A}}^{-1})^\top \\ u \end{pmatrix} - \mathbf{c}_1^\top \mathbf{t} \\
&= \bar{\mathbf{c}}_0^\top (\overline{\mathbf{A}}^{-1})^\top \sum f'_i(\mathsf{id})\mathbf{z}'_i + (\underline{\mathbf{c}}_0^\top - (\underline{\mathbf{A}}\overline{\mathbf{A}}^{-1}\bar{\mathbf{c}}_0)^\top)u + ((\sum f_i(\mathsf{id})\mathbf{Z}_i \cdot \overline{\mathbf{A}}^{-1} \cdot \bar{\mathbf{c}}_0)^\top - \mathbf{c}_1^\top)\mathbf{t} \\
&= \bar{\mathbf{c}}_0^\top (\overline{\mathbf{A}}^{-1})^\top \sum f'_i(\mathsf{id})\mathbf{z}'_i + (\underline{\mathbf{c}}_0^\top - (\underline{\mathbf{A}}\overline{\mathbf{A}}^{-1}\bar{\mathbf{c}}_0)^\top) \sum f'_i(\mathsf{id})x'_i \qquad \text{(substituting } u\text{)} \\
&\quad + \underbrace{((\underline{\mathbf{c}}_0^\top - (\underline{\mathbf{A}}\overline{\mathbf{A}}^{-1}\bar{\mathbf{c}}_0)^\top) \sum f_i(\mathsf{id})\mathbf{x}_i^\top + (\sum f_i(\mathsf{id})\mathbf{Z}_i \cdot \overline{\mathbf{A}}^{-1} \cdot \bar{\mathbf{c}}_0)^\top - \mathbf{c}_1^\top)\mathbf{t}}_{E}
\end{aligned}
$$

INITIALIZE:
$\mathbf{A} \xleftarrow{\$} \mathcal{D}_k$
$\varepsilon \xleftarrow{\$}$ INITIALIZE$_{\mathsf{MAC}}$
For $i = 0, \ldots, \ell$: $\mathbf{Z}_i \xleftarrow{\$} \mathbb{Z}_q^{n \times k}$
For $i = 0, \ldots, \ell'$: $\mathbf{z}'_i \xleftarrow{\$} \mathbb{Z}_q^{1 \times k}$
$\mathsf{pk} := (\mathcal{G}, [\mathbf{A}]_1, ([\mathbf{Z}_i]_1)_{0 \le i \le \ell}, ([\mathbf{z}'_i]_1)_{0 \le i \le \ell'})$
Return pk

ENC(id^*): //one query
$([h]_1, [\mathbf{h}_0[\mathsf{id}^*] \cdot h]_1) \xleftarrow{\$}$ CHAL(id^*)
$\overline{\mathbf{c}}_0^* \xleftarrow{\$} \mathbb{Z}_q^k$; $\underline{\mathbf{c}}_0^* = h + \underline{\mathbf{A}} \cdot \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}}_0^* \in \mathbb{Z}_q$
$\mathbf{c}_1^* = \sum_{i=0}^{\ell} f_i(\mathsf{id}^*) \mathbf{Z}_i \cdot \overline{\mathbf{A}}^{-1} \overline{\mathbf{c}}_0^* + \mathbf{h}_0[\mathsf{id}^*] \cdot h$
Return $\mathsf{C}^* = ([\mathbf{c}_0^*]_1, [\mathbf{c}_1^*]_1)$

USKGEN(id):
If $\mathsf{usk}[\mathsf{id}] = \perp$ then
$([\mathbf{t}]_2, [u]_2) \xleftarrow{\$}$ EVAL(id)
$\mathbf{v}^\top = (\mathbf{t}^\top \sum f_i(\mathsf{id}) \mathbf{Z}_i + \sum f'_i(\mathsf{id}) \mathbf{z}'_i - u \cdot \underline{\mathbf{A}}) \cdot \overline{\mathbf{A}}^{-1}$
$\mathsf{usk}[\mathsf{id}] := ([\mathbf{t}]_2, [u]_2, [\mathbf{v}]_2) \in \mathbb{G}_2^n \times \mathbb{G}_2^1 \times \mathbb{G}_2^k$
$\mathcal{Q}_{\mathcal{ID}} = \mathcal{Q}_{\mathcal{ID}} \cup \{(\mathsf{id}, \mathsf{usk}[\mathsf{id}])\}$
Return $\mathsf{usk}[\mathsf{id}]$

Figure 26: Description of $\mathcal{B}_2$ (having access to the oracles INITIALIZE$_{\mathsf{MAC}}$, EVAL, CHAL, FINALIZE$_{\mathsf{MAC}}$ of the $\mathsf{PR\text{-}CMA_{real}}/\mathsf{PR\text{-}CMA_{rand}}$ games of Figure 24) for the proof of Lemma C.10.

Since $(\mathbf{c}_0, \mathbf{c_1})$ from Encap^* is chosen uniformly at random, $\mathbf{c}_1^\top \neq (\underline{\mathbf{c}}_0^\top - (\underline{\mathbf{A}}\overline{\mathbf{A}}^{-1}\overline{\mathbf{c}}_0)^\top) \sum f_i(\mathsf{id})\mathbf{x}_i^\top + (\sum f_i(\mathsf{id})\mathbf{Z}_i \cdot \overline{\mathbf{A}}^{-1} \cdot \overline{\mathbf{c}}_0)^\top$ with probability $1 - 1/q^n$. Conditioned on that and since $\mathrm{rank}(\mathbf{B}) \ge 1$ and $\mathbf{t} = \mathbf{B}\mathbf{s}$ (for $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^{n'}$), E is uniformly random. This concludes the theorem. ∎

D Concrete Instantiation from SXDH

We now describe our tightly PR-ID-CPA-secure IBKEM $\mathsf{IBKEM}[\mathsf{MAC_{NR}}[\mathcal{D}_k], \mathcal{U}_1]$ for the special case of $k = 1$ and $\mathcal{D}_k = \mathcal{U}_1$, such that $\mathcal{D}_k$-MDDH is the DDH assumption. The identity space is $\mathcal{ID} = \{0,1\}^\ell$. Theorems 4.3 and 3.3 provide a tight security reduction under the the DDH assumptions in $\mathbb{G}_1$ and $\mathbb{G}_2$, i.e., under the SXDH assumption.

$\mathsf{Gen}(\mathsf{par})$:
$\mathsf{sk_{MAC}} = (x_0, \ldots, x_\ell, x') \xleftarrow{\$} \mathbb{Z}_q^{\ell+2}$
$a \xleftarrow{\$} \mathbb{Z}_q$
For $i = 0, \ldots, \ell : y_i \xleftarrow{\$} \mathbb{Z}_q; z_i = a y_i + x_i \in \mathbb{Z}_q$
$y' \xleftarrow{\$} \mathbb{Z}_q; z' = a y' + x' \in \mathbb{Z}_q$
$\mathsf{pk} := (\mathcal{G}, [a]_1, ([z_i]_1)_{0 \le i \le \ell}, [z']_1)$
$\mathsf{sk} := (\mathsf{sk_{MAC}}, (y_i)_{0 \le i \le \ell}, y')$
Return $(\mathsf{pk}, \mathsf{sk})$.

$\mathsf{USKGen}(\mathsf{sk}, \mathsf{id})$:
$t \xleftarrow{\$} \mathbb{Z}_q$
$u = x' + t(x_0 + \sum_{i=1}^{\ell} \mathsf{id}_i \cdot x_i)$
$v = y' + t(y_0 + \sum_{i=1}^{\ell} \mathsf{id}_i \cdot y_i)$
Return $\mathsf{usk}[\mathsf{id}] := ([t]_2, [u]_2, [v]_2) \in \mathbb{G}_2^3$

$\mathsf{Enc}(\mathsf{pk}, \mathsf{id})$:
$r \xleftarrow{\$} \mathbb{Z}_q$
$\mathbf{c}_0 := (c_{0,0}, c_{0,1}) = (r, a \cdot r)$
$c_1 = r(z_0 + \sum_{i=1}^{\ell} \mathsf{id}_i z_i)$
$K = z' \cdot r$.
Return $\mathsf{K} = [K]_T$ and $\mathsf{C} = ([\mathbf{c}_0]_1, [c_1]_1) \in \mathbb{G}_1^3$.

$\mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id}, \mathsf{C})$:
Parse $\mathsf{usk}[\mathsf{id}] = ([t]_2, [u]_2, [v]_2)$
Parse $\mathsf{C} = ([\mathbf{c}_0]_1, [c_1]_1)$
$\mathsf{K} = e([c_{0,0}]_1, [v]_2) \cdot e([c_{0,1}]_1, [u]_2) / e([c_1]_1, [t]_2)$
Return $\mathsf{K} \in \mathbb{G}_T$.

$\mathsf{IBKEM}[\mathsf{MAC_{NR}}[\mathcal{D}_k], \mathcal{U}_1]$ is a "Cramer-Shoup variant" of Waters' IBKEM Wat05 [30]. Concretely, Wat05 is a projected variant of our scheme and is obtained by setting $\mathsf{usk}[\mathsf{id}] := ([t]_2, [u + av]_2) \in \mathbb{G}_2^2$ and $\mathsf{C} = ([c_0 = \mathbf{c}_{0,0} + a\mathbf{c}_{0,1}], [c_1]) \in \mathbb{G}_1^2$. Wat05 is IND-ID-CPA-secure under the CDH assumption, with a non-tight security proofs. See [3] for a discussion on the impact of the non-tight reduction. Our IBKEM is tightly IND-ID-CPA-secure and anonymous under the SXDH assumption.