(Hierarchical) Identity-Based Encryption from Affine Message Authentication

Olivier Blazy, Eike Kiltz, and 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 the first tightly secure HIBE in the standard model.

Keywords: IBE, HIBE, standard model, tight reduction.

1 Introduction

Identity-based encryption (IBE) [24] enables a user to encrypt to a recipient's identity id (e.g., an email or phone number); decryption can be done using a user secret key for id, obtained from a trusted authority. The first instantiations of an IBE scheme were given in 2001 [7,4,23]. Whereas earlier constructions relied on the random oracle model, the first adaptively secure construction in the standard model was proposed in [26]. 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 [26] 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

J.A. Garay and R. Gennaro (Eds.): CRYPTO 2014, Part I, LNCS 8616, pp. 408–425, 2014.

[25,6] only lose a factor Q, independent of L. The first tightly secure IBE was recently proposed by Chen and Wee [6] 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 [9] and an old construction by Bellare and Goldwasser [1] 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 [6] 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 $[\mathbf{a}] := g^{\mathbf{a}} = (g^{\mathbf{a}_1}, \ldots, g^{\mathbf{a}_n})^\top \in \mathbb{G}^n$ 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 [10], as well as the MAC derived from the randomized Naor-Reingold PRF [21] implicitly given in [6] are affine.

From Affine MACs to 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 [11][1] 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 $\mathsf{PR\text{-}CMA}$-secure (pseudorandom against chosen message attacks,

[1] 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 ($k = 1$).

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 $\mathsf{HIBE}[\mathsf{MAC}_n, \mathcal{D}_k]$. If the affine MAC is furthermore *anonymity-preserving*, 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 $\mathsf{HIBE}[\mathsf{MAC}_n, \mathcal{D}_k]$. Due to space restrictions, the anonymity-preserving transformation $\mathsf{AHIBE}[\mathsf{MAC}_n, \mathcal{D}_k]$ is only given in the full version [3].

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 Delegatable Affine MACs. To instantiate our transformations, we consider two specific delegatable affine MACs. Our first construction, $\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k]$, is a generalization of the MAC derived from the randomized Naor-Reingold PRF [6] to any $\mathcal{D}_k$-MDDH Assumption. (Unfortunately, the MAC based on the original deterministic Naor-Reingold PRF is not affine.) We show that it is affine over $\mathbb{Z}_q^n$ with $n = k$ and delegatable. We prove 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 the first HIBE with a tight security reduction to a standard assumption. Ciphertexts and user secret keys of $\mathsf{HIBE}[\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k], \mathcal{D}_k]$ 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 can be seen as a "two-copy version" of Waters' IBE [26] 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 [11] for any $\mathcal{D}_k$-MDDH problem. A hash proof system is known to imply a UF-CMA-secure MAC [10]. 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 [6]. Additionally, we show $\mathsf{MAC}_{\mathsf{HPS}}[\mathcal{D}_k]$ is also anonymity-preserving, which implies an anonymous (but non-tight) HIBE, $\mathsf{AHIBE}[\mathsf{MAC}_{\mathsf{HPS}}[\mathcal{D}_k], \mathcal{D}_k]$, while the delegatable $\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k]$ is unlikely to be anonymity-preserving.

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 a chosen-ciphertext secure (H)IBE [16]. Furthermore, any (H)IBE directly implies a (Hierarchical ID-based) signature scheme [12]. 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 [14,2].

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 transfor-

Table 1. Comparison between known adaptively secure IBEs with identity-space $\mathcal{ID} = \{0,1\}^\lambda$ and L-level HIBEs with identity-space $\mathcal{ID} = (\{0,1\}^\lambda)^L$ in prime order groups from standard assumptions. For $|\mathsf{pk}|$ (public-key size), $|\mathsf{usk}|$ (user secret-key size), and $|\mathsf{C}|$ (ciphertext size), we count the sum of all elements in $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$, and $\mathbb{Z}_q$. Q is the number of user secret key queries by the adversary. Schemes from this paper are: $\mathsf{IBE}_{\mathsf{HPS}} := \mathsf{IBE}[\mathsf{MAC}_{\mathsf{HPS}}[\mathcal{D}_k], k\text{-LIN}]$, $\mathsf{IBE}_{\mathsf{NR}} := \mathsf{IBE}[\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k], k\text{-LIN}]$, $\mathsf{HIBE}_{\mathsf{HPS}} := \mathsf{HIBE}[\mathsf{MAC}_{\mathsf{HPS}}[\mathcal{D}_k], k\text{-LIN}]$, $\mathsf{HIBE}_{\mathsf{NR}} := \mathsf{HIBE}[\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k], k\text{-LIN}]$ and $\mathsf{AHIBE}_{\mathsf{HPS}} := \mathsf{AHIBE}[\mathsf{MAC}_{\mathsf{HPS}}[\mathcal{D}_k], k\text{-LIN}]$.

	Scheme	$\lvert\mathsf{pk}\rvert$	$\lvert\mathsf{usk}\rvert$	$\lvert\mathsf{C}\rvert$	Anonymity?	Loss	Assumption
IBE	Wat05 [26]	$4 + \lambda$	2	2	–	$O(\lambda Q)$	DBDH
	Wat09 [25]	13	9	10	–	$O(Q)$	2-LIN
	Lew12 [17]	25	6	6	$\surd$	$O(Q)$	2-LIN
	CLL$^+$12 [5]	9	4	4	–	$O(Q)$	SXDH
	JR13 [15]	7	5	4	–	$O(Q)$	SXDH
	CW13 [6]	$2k^2(2\lambda + 1) + k$	$4k$	$4k$	–	$O(\lambda)$	k-LIN
	$\mathsf{IBE}_{\mathsf{HPS}}$	$3k^2 + 4k$	$2k + 2$	$2k + 2$	$\surd$	$O(Q)$	k-LIN
	$\mathsf{IBE}_{\mathsf{NR}}$	$2\lambda k^2 + 2k$	$2k + 1$	$2k + 1$	$\surd$	$O(\lambda)$	k-LIN
HIBE	Wat05 [26]	$O(\lambda L)$	$O(\lambda L)$	$1 + L$	–	$O(\lambda Q)^L$	DBDH
	Wat09 [25]	$O(L)$	$O(L)$	$O(L)$	–	$O(Q)$	2-LIN
	CW13 [6]	$O(Lk^2)$	$O(Lk)$	$2k + 2$	–	$O(Q)$	k-LIN
	$\mathsf{HIBE}_{\mathsf{HPS}}$	$O(Lk^2)$	$O(Lk)$	$2k + 2$	–	$O(Q)$	k-LIN
	$\mathsf{HIBE}_{\mathsf{NR}}$	$O(L\lambda k^2)$	$O(L\lambda k)$	$2k + 1$	–	$O(L\lambda)$	k-LIN
	$\mathsf{AHIBE}_{\mathsf{HPS}}$	$O(Lk^2)$	$O(Lk^2)$	$2k + 2$	$\surd$	$O(Q)$	k-LIN

mation from Bellare and Goldwasser [1] 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 [13] 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 [8], 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 [27] proposed an information-theoretic primitive called *predicate encodings* that characterize the underlying algebraic structure of a number of predicate encoding schemes, including known IBE [19] and attribute-based encryption (ABE) [18] 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 [25] 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 [25,19,6] 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 [15]. 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".

Lewko and Waters [20] consider the difficulty of a security proof for L-level HIBEs that does not proving exponentially in L. Essentially, they prove that any scheme with rerandomizable user secret keys (over the space of all "functional" user secret keys) will suffer an exponential degradation in security. While some of our tightly-secure HIBEs are rerandomizable, they are only rerandomizable over the space of all user secret keys generated by the user secret key generation algorithm. Hence, our tightly-secure HIBE does not contradict the negative results of [20].

1.4 Open Problems

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

2 Definitions

2.1 Notation

If $\mathbf{x} \in \mathcal{B}^n$, then $|\mathbf{x}|$ denotes the length n of the vector. Further, $x \leftarrow_{\$} \mathcal{B}$ denotes the process of sampling an element x from set $\mathcal{B}$ uniformly at random.

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 $\mathcal{G} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, g_1, g_2, e)$ 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, g_1 and g_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 $g_T := e(g_1, g_2)$, which is a generator in $\mathbb{G}_T$.

We use implicit representation of group elements as introduced in [11]. For $s \in \{1, 2, T\}$ and $a \in \mathbb{Z}_q$ define $[a]_s = g_s^a \in \mathbb{G}_s$ 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 $\mathbb{G}_s$:

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

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 [11].

Definition 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 $\mathbf{A} \leftarrow_\$ \mathcal{D}_k$ form an invertible matrix. The $\mathcal{D}_k$-Matrix Diffie-Hellman problem is to distinguish the two distributions $([\mathbf{A}], [\mathbf{A}\mathbf{w}])$ and $([\mathbf{A}], [\mathbf{u}])$ where $\mathbf{A} \leftarrow_\$ \mathcal{D}_k$, $\mathbf{w} \leftarrow_\$ \mathbb{Z}_q^k$ and $\mathbf{u} \leftarrow_\$ \mathbb{Z}_q^{k+1}$.

Definition 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 $\mathcal{D}$,*

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

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

For each $k \geq 1$, [11] 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 of $\mathbf{A}$ are exemplified for $k = 2$, where $a_1, \ldots, a_6 \leftarrow_\$ \mathbb{Z}_q$.

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

It was also shown in [11] 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.

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 $\mathsf{sk}_{\mathsf{MAC}} \leftarrow_\$ \mathsf{Gen}_{\mathsf{MAC}}(\mathsf{par})$ returns a secret key, $\tau \leftarrow_\$ \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m})$ 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. *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* $n', \ell, \ell' \in \mathbb{N}$.
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*

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

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

   for some public defining functions $f_i : \mathcal{M} \to \mathbb{Z}_q$ *and* $f'_i : \mathcal{M} \to \mathbb{Z}_q$. *Vector* $\mathbf{t}$ *is the randomness 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 (3) holds.*

The standard security notion for probabilistic MACs is unforgeability against chosen-message attacks UF-CMA [10]. In this work we require *pseudorandom 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 $\mathbb{G}_T$.

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

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

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 $\mathsf{PR\text{-}CMA}_{\mathsf{real}}$ and $\mathsf{PR\text{-}CMA}_{\mathsf{rand}}$ from Figure 1. Note that the output $([h]_1, [\mathbf{h}_0]_1, [h_1]_T)$ of CHAL(m^*) in game $\mathsf{PR\text{-}CMA}_{\mathsf{real}}$ 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 4. *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. We use the following randomized version $\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k] = (\mathsf{Gen}_{\mathsf{MAC}}, \mathsf{Tag}, \mathsf{Ver})$ 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 [6]. For a 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 $\underline{\mathbf{A}} \in \mathbb{Z}_q^{1\times k}$.

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

Note that $\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k]$ 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 $1 \le i \le m$, where m_i is the i-th bit of 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.)

Theorem 1. $\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k]$ *is tightly* 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* $\mathsf{Adv}^{\mathsf{pr\text{-}cma}}_{\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k]}(\mathcal{A}) \le 4m(\mathbf{Adv}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{D}) - 1/(q-1))$.

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 [6,22]. 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 [11] (which gives Q-many real-or-random $\mathcal{D}_k$-MDDH tuples) 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 [11], the proof follows. A formal proof can be found in the full version [3].

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 Sect. 5.)

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 [11] with the generic MAC construction from [10] and obtain the following $\mathsf{MAC}_{\mathsf{HPS}}[\mathcal{D}_k]$ for $\mathcal{M} = \mathbb{Z}_q^\ell$. Algorithm $\mathsf{Gen}_{\mathsf{MAC}}(\mathsf{par})$ picks $\mathbf{B} \leftarrow_\$ \mathcal{D}_k$, $\mathbf{x}_0, \ldots, \mathbf{x}_\ell \leftarrow_\$ \mathbb{Z}_q^{k+1}$, and $x'_0 \leftarrow_\$ \mathbb{Z}_q$. The MAC secret-key is $\mathsf{sk}_{\mathsf{MAC}} = (\mathbf{B}, \mathbf{x}_0, \ldots, \mathbf{x}_\ell, x'_0)$.

$\underline{\mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m})}$:	$\underline{\mathsf{Ver}(\mathsf{sk}_{\mathsf{MAC}}, \tau, \mathsf{m})}$:
Parse $\mathsf{sk}_{\mathsf{MAC}} = (\mathbf{B}, \mathbf{x}_0, \ldots, \mathbf{x}_\ell, x'_0)$	Parse $\mathsf{sk}_{\mathsf{MAC}} = (\mathbf{B}, \mathbf{x}_0, \ldots, \mathbf{x}_\ell, x'_0)$
$\mathbf{s} \leftarrow_\$ \mathbb{Z}_q^k$; $\mathbf{t} = \mathbf{B}\mathbf{s} \in \mathbb{Z}_q^{k+1}$	If $u = (\mathbf{x}_0^\top + \sum_{i=1}^{\lvert\mathsf{m}\rvert} \mathsf{m}_i \cdot \mathbf{x}_i^\top)\mathbf{t} + x'_0$
$u = (\mathbf{x}_0^\top + \sum_{i=1}^{\lvert\mathsf{m}\rvert} \mathsf{m}_i \cdot \mathbf{x}_i^\top)\mathbf{t} + x'_0$	then return 1
Return $\tau = ([\mathbf{t}]_2, [u]_2) \in \mathbb{G}_2^{k+1} \times \mathbb{G}_2$	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 [11,10] 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. A formal proof can be found in the full version [3].

Theorem 2. $\mathsf{MAC}_{\mathsf{HPS}}[\mathcal{D}_k]$ *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* $\textsc{Eval}(\cdot)$.

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 5 (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 a message space* $\mathcal{M}$*, 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* $\mathsf{Enc}(\mathsf{pk}, \mathsf{id})$*:*

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

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 2.

Definition 6 (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.*

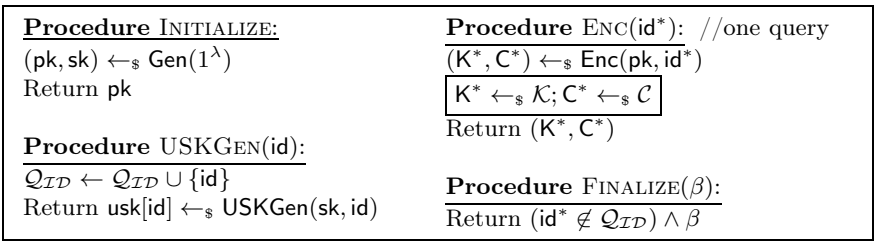

Fig. 2. Security Games $\mathsf{PR\text{-}ID\text{-}CPA}_{\mathsf{real}}$ and $\boxed{\mathsf{PR\text{-}ID\text{-}CPA}_{\mathsf{rand}}}$ for defining PR-ID-CPA-security

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 in Figure 3.

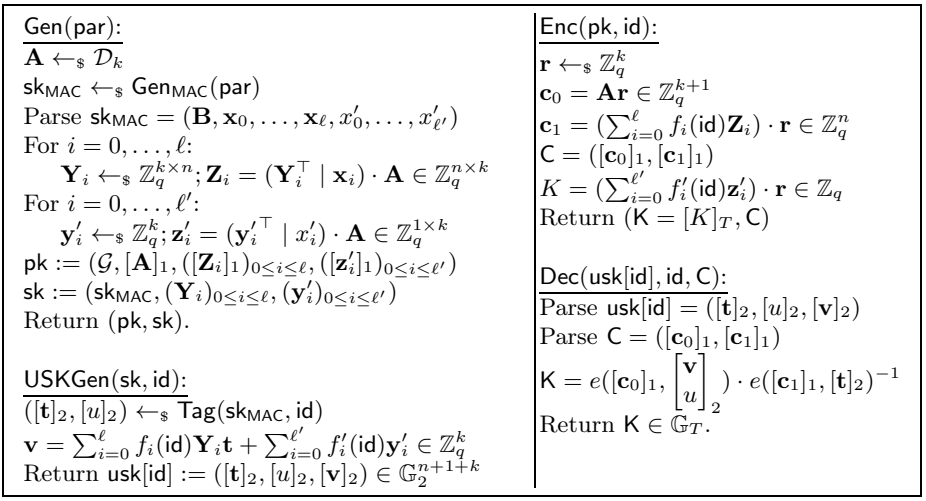

Fig. 3. Definition of the transformation $\mathsf{IBKEM}[\mathsf{MAC}, \mathcal{D}_k]$

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 $\mathsf{sk}_{\mathsf{MAC}} = (\mathbf{x}_1, \ldots, \mathbf{x}_\ell, \mathbf{x}'_1, \ldots, \mathbf{x}'_{\ell'})$ of MAC. User secret key generation computes the MAC tag $\tau = ([\mathbf{t}]_2, [u]_2) \leftarrow_{\$} \mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}})$ 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 output of $\mathsf{USKGen}(\mathsf{sk}, \mathsf{id})$. By Equation (3) in Section 3, we have

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

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

Theorem 3. *Under the* $\mathcal{D}_k$-MDDH *assumption relative to* GGen *in* $\mathbb{G}_1$ *and the* $\mathsf{PR\text{-}CMA}$*-security of* MAC*,* $\mathsf{IBKEM}[\mathsf{MAC}, \mathcal{D}_k]$ *is a* $\mathsf{PR\text{-}ID\text{-}CPA}$*-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* $\mathsf{Adv}^{\mathsf{pr\text{-}id\text{-}cpa}}_{\mathsf{IBKEM}[\mathsf{MAC},\mathcal{D}_k]}(\mathcal{A}) \leq \mathbf{Adv}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}_1) + \mathsf{Adv}^{\mathsf{pr\text{-}cma}}_{\mathsf{MAC}}(\mathcal{B}_2)$.

The proof can be found in the full version [3].

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. In the full version [3] we recall syntax and $\mathsf{IND\text{-}HID\text{-}CPA}$ security of a hierarchical ID-based key encapsulation mechanism (HIBKEM).

5.1 Delegatable Affine MACs

Definition 7. *An affine* MAC *over* $\mathbb{Z}_q^n$ *(Definition 3) is* delegatable*, if the message space is* $\mathcal{M} = \mathcal{B}^{\leq m}$ *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* $l(\mathsf{m}) \leq l(\mathsf{m}')$ *and*

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

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

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

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 $\mathcal{M} = \mathcal{B}^{\leq m} := \bigcup_{i=1}^{m} \mathcal{B}^i$. To build a HIBE, we require a new notion denoted as $\mathsf{HPR_0\text{-}CMA}$ security. It differs from $\mathsf{PR\text{-}CMA}$ 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 4.

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

Fig. 4. Games $\mathsf{HPR\text{-}CMA}_{\mathsf{real}}$, and $\boxed{\mathsf{HPR_0\text{-}CMA}_{\mathsf{rand}}}$ for defining $\mathsf{HPR_0\text{-}CMA}$ security

Definition 8. *A delegatable affine* MAC *over* $\mathbb{Z}_q^n$ *is* $\mathsf{HPR_0\text{-}CMA}$*-secure if for all PPT* $\mathcal{A}$, $\mathsf{Adv}^{\mathsf{hpr_0\text{-}cma}}_{\mathsf{MAC}}(\mathcal{A}) := \Pr[\mathsf{HPR\text{-}CMA}^{\mathcal{A}}_{\mathsf{real}} \Rightarrow 1] - \Pr[\mathsf{HPR_0\text{-}CMA}^{\mathcal{A}}_{\mathsf{rand}} \Rightarrow 1]$ *is negligible.*

5.2 Examples of Delegatable Affine MACs

We first note that $\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k]$ from Section 3 with message space $\mathcal{M} = \{0,1\}^{\leq m}$ is delegatable.

Theorem 4. *Under the* $\mathcal{D}_k$-MDDH *assumption,* $\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k]$ *is tightly* $\mathsf{HPR_0\text{-}CMA}$ *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* $\mathsf{Adv}^{\mathsf{hpr_0\text{-}cma}}_{\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k]}(\mathcal{A}) \leq 6m(\mathbf{Adv}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{D}) - 1/(q-1))$.

The proof is similar to that of Theorem 1, with the difference that the reduction between games G_i and G_{i-1} now has to guess $\mathsf{m}_i^* \in \{0, 1, \perp\}$, where $\perp$ means that $|\mathsf{m}^*| < i$. Furthermore, $\mathbf{h}_0$ from CHAL(m^*) is not pseudorandom in the delegatable case, since $([\mathbf{B}]_2, ([\mathbf{x}_i^\top \mathbf{B}]_2)_{0\leq i\leq m})$ are disclosed from INITIALIZE and

then it is easy to check if $\mathbf{h}_0$ is well-formed under m^* by using the pairing. A formal proof of Theorem 4 is given in [3].

We now turn to $\mathsf{MAC}_{\mathsf{HPS}}[\mathcal{D}_k]$ from Section 3 with message space $\mathcal{M} = \mathcal{B}^{\leq m} = (\mathbb{Z}_q^*)^{\leq m}$. Again, it can be verified to be 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 $\mathsf{m}\|0$.

Theorem 5. *Under the* $\mathcal{D}_k$-MDDH *assumption,* $\mathsf{MAC}_{\mathsf{HPS}}[\mathcal{D}_k]$ *is* 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* $\mathsf{Adv}^{\mathsf{hpr}_0\text{-}\mathsf{cma}}_{\mathsf{MAC}_{\mathsf{HPS}}[\mathcal{D}_k]}(\mathcal{A}) \leq 2Q(\mathbf{Adv}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{D}) + 1/q)$*, where* Q *is the maximal number of queries to* $\textsc{Eval}(\cdot)$*.*

A formal proof can be found in the full version [3].

5.3 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 $\mathcal{M} = \mathcal{B}^{\leq m}$. 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 $\mathcal{ID} = \mathcal{M} = \mathcal{B}^{\leq m}$ is defined as in Figure 5. Compared to the IBE construction from Section 4, the main difference is that Gen also returns a delegation key dk which allows re-randomization of every $\mathsf{usk}[\mathsf{id}]$. Further, USKGen also outputs user delegation keys $\mathsf{udk}[\mathsf{id}]$ 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, $\mathsf{usk}[\mathsf{id}']$ 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 our construction is a $\mathsf{IND\text{-}HID\text{-}CPA}$-secure HIBKEM. Its proof can be found in [3]. 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 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*

$$\mathsf{Adv}^{\mathsf{ind\text{-}hid\text{-}cpa}}_{\mathsf{HIBKEM}[\mathsf{MAC},\mathcal{D}_k]}(\mathcal{A}) \leq \mathbf{Adv}_{\mathcal{D}_k,\mathsf{GGen}}(\mathcal{B}_1) + \mathsf{Adv}^{\mathsf{hpr}_0\text{-}\mathsf{cma}}_{\mathsf{MAC}}(\mathcal{B}_2).$$

$\underline{\mathsf{Gen}(\mathsf{par})}$:
$\mathbf{A} \leftarrow_\$ \mathcal{D}_k$; $\mathsf{sk}_{\mathsf{MAC}} \leftarrow_\$ \mathsf{Gen}_{\mathsf{MAC}}(\mathsf{par})$
Parse $\mathsf{sk}_{\mathsf{MAC}} = (\mathbf{B}, \mathbf{x}_0, \ldots, \mathbf{x}_\ell, x'_0, \ldots, x'_{\ell'})$
For $i = 0, \ldots, \ell$:
$\mathbf{Y}_i \leftarrow_\$ \mathbb{Z}_q^{k \times n}$; $\mathbf{Z}_i = (\mathbf{Y}_i^\top \mid \mathbf{x}_i) \cdot \mathbf{A} \in \mathbb{Z}_q^{n \times k}$
$\mathbf{d}_i = \mathbf{x}_i^\top \cdot \mathbf{B} \in \mathbb{Z}_q^{n'}$; $\mathbf{E}_i = \mathbf{Y}_i \cdot \mathbf{B} \in \mathbb{Z}_q^{k \times n'}$
$\mathbf{y}'_0 \leftarrow_\$ \mathbb{Z}_q^k$; $\mathbf{z}'_0 = (\mathbf{y}'^\top_0 \mid x'_0) \cdot \mathbf{A} \in \mathbb{Z}_q^{1 \times k}$
$\mathsf{pk} := (\mathcal{G}, [\mathbf{A}]_1, ([\mathbf{Z}_i]_1)_{0 \le i \le \ell}, [\mathbf{z}'_0]_1)$
$\mathsf{dk} := ([\mathbf{B}]_2, ([\mathbf{d}_i]_2, [\mathbf{E}_i]_2)_{0 \le i \le \ell})$
$\mathsf{sk} := (\mathsf{sk}_{\mathsf{MAC}}, (\mathbf{Y}_i)_{0 \le i \le \ell}, \mathbf{y}'_0)$
Return $(\mathsf{pk}, \mathsf{dk}, \mathsf{sk})$

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

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

$\underline{\mathsf{USKDel}(\mathsf{usk}[\mathsf{id}], \mathsf{udk}[\mathsf{id}], \mathsf{id}, \mathsf{id}_{p+1})}$:
Parse $\mathsf{id} \in \mathcal{B}^p, \mathsf{id}_{p+1} \in \mathcal{B}$
$\mathsf{id}' := (\mathsf{id}_1, \ldots, \mathsf{id}_p, \mathsf{id}_{p+1}) \in \mathcal{B}^{p+1}$
If $p \ge m$, then return $\perp$
//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 $\hat{\mathbf{v}}$:
$\mathbf{s}' \leftarrow_\$ \mathbb{Z}_q^{n'}$
$\mathbf{t}' = \mathbf{t} + \mathbf{B}\mathbf{s}' \in \mathbb{Z}_q^n$
$u' = \hat{u} + \sum_{i=0}^{l(\mathsf{id}')} f_i(\mathsf{id}') \mathbf{d}_i \mathbf{s}' \in \mathbb{Z}_q$
$\mathbf{v}' = \hat{\mathbf{v}} + \sum_{i=0}^{l(\mathsf{id}')} f_i(\mathsf{id}') \mathbf{E}_i \mathbf{s}' \in \mathbb{Z}_q^k$
//Rerandomization of d'_i and $\mathbf{e}_i$:
For $i = l(\mathsf{id}') + 1, \ldots, \ell$:
$d'_i = d_i + \mathbf{d}_i \mathbf{s}' \in \mathbb{Z}_q$
$\mathbf{e}'_i = \mathbf{e}_i + \mathbf{E}_i \mathbf{s}' \in \mathbb{Z}_q^k$
$\mathsf{usk}[\mathsf{id}'] := ([\mathbf{t}']_2, [u]_2, [\mathbf{v}']_2)$
$\mathsf{udk}[\mathsf{id}'] := ([d'_i]_2, [\mathbf{e}'_i]_2)_{l(\mathsf{id}') < i \le \ell}$
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 $\mathsf{C} = ([\mathbf{c}_0]_1, [\mathbf{c}_1]_1)$
$\mathsf{K} = e([\mathbf{c}_0]_1, \begin{bmatrix} \mathbf{v} \\ u \end{bmatrix}_2) \cdot e([\mathbf{c}_1]_1, [\mathbf{t}]_2)^{-1}$
Return $\mathsf{K} \in \mathbb{G}_T$

Fig. 5. Definition of the transformation $\mathsf{HIBKEM}[\mathsf{MAC}, \mathcal{D}_k]$

5.4 Anonymity-Preserving Transformation

In this section, we sketch an alternative (but less efficient) transformation, which is anonymity-preserving. Due to space limitations, we only give the idea behind our construction and refer to the full version for details.

Our transformation is based on the notion of APR-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 HPR-CMA-security (Section 5.1) in the sense that $\textsc{Eval}(\mathsf{m})$ will output the terms for usk rerandomization, not $\textsc{Initialize}$ and that in the random game, $\textsc{Chal}$ returns uniform $(\mathbf{h}_0, h_1)$. Unfortunately, $\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k]$ is unlikely to be APR-CMA-secure, but $\mathsf{MAC}_{\mathsf{HPS}}[\mathcal{D}_k]$ with message space $\mathcal{M} = \mathcal{B}^{\le m} = (\mathbb{Z}_q^*)^{\le m}$ is provably APR-CMA-secure.

Compared to the HIBE construction from Section 5.3, the new transformation $\mathsf{AHIBKEM}[\mathsf{MAC}, \mathcal{D}_k]$ uses a different rerandomization method for usk :=

$([\mathbf{t}]_2, [u]_2, [\mathbf{v}]_2)$: USKGen outputs a random basis $\mathbf{T}$ which allows rerandomization of $\mathbf{t}$; similarly, $\mathbf{u}$ and $\mathbf{V}$ are generated for rerandomizing u and $\mathbf{v}$. In the full version we prove that if MAC is an $\mathsf{APR\text{-}CMA}$-secure and the $\mathcal{D}_k$-MDDH assumption holds in $\mathbb{G}_1$, then $\mathsf{AHIBKEM}[\mathsf{MAC}, \mathcal{D}_k]$ is $\mathsf{PR\text{-}HID\text{-}CPA}$-secure, i.e., $\mathsf{IND\text{-}HID\text{-}CPA}$-secure and anonymous.

Acknowledgements. All authors were (partially) supported by the Sofja Kovalevskaja Award of the Alexander von Humboldt Foundation and the German Federal Ministry for Education and Research. Jiaxin Pan was also partially supported by the German Israel Foundation.

We thank Hoeteck Wee for various comments and helpful discussions.

References

1. Bellare, M., Goldwasser, S.: New paradigms for digital signatures and message authentication based on non-interactive zero knowledge proofs. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 194–211. Springer, Heidelberg (1990)
2. Blazy, O., Kakvi, S., Kiltz, E., Pan, J.: Tightly-secure signatures from chameleon hash functions. unpublished (2013)
3. Blazy, O., Kiltz, E., Pan, J.: (Hierarchical) identity-based encryption from affine message authentication. Cryptology ePrint Archive, Full version of this paper (2014)
4. Boneh, D., Franklin, M.: Identity-based encryption from the Weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)
5. Chen, J., Lim, H.W., Ling, S., Wang, H., Wee, H.: Shorter IBE and signatures via asymmetric pairings. In: Abdalla, M., Lange, T. (eds.) Pairing 2012. LNCS, vol. 7708, pp. 122–140. Springer, Heidelberg (2013)
6. Chen, J., Wee, H.: Fully (almost) tightly secure IBE and dual system groups. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part II. LNCS, vol. 8043, pp. 435–460. Springer, Heidelberg (2013)
7. Cocks, C.: An identity based encryption scheme based on quadratic residues. In: Honary, B. (ed.) Cryptography and Coding 2001. LNCS, vol. 2260, pp. 360–363. Springer, Heidelberg (2001)
8. Cramer, R., Shoup, V.: A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 13–25. Springer, Heidelberg (1998)
9. Cramer, R., Shoup, V.: Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 45–64. Springer, Heidelberg (2002)
10. Dodis, Y., Kiltz, E., Pietrzak, K., Wichs, D.: Message authentication, revisited. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 355–374. Springer, Heidelberg (2012)
11. Escala, A., Herold, G., Kiltz, E., Ràfols, C., Villar, J.: An algebraic framework for Diffie-Hellman assumptions. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part II. LNCS, vol. 8043, pp. 129–147. Springer, Heidelberg (2013)
12. Gentry, C., Silverberg, A.: Hierarchical ID-based cryptography. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 548–566. Springer, Heidelberg (2002)

13. Groth, J., Sahai, A.: Efficient non-interactive proof systems for bilinear groups. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 415–432. Springer, Heidelberg (2008)
14. Hofheinz, D., Jager, T.: Tightly secure signatures and public-key encryption. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 590–607. Springer, Heidelberg (2012)
15. Jutla, C.S., Roy, A.: Shorter quasi-adaptive NIZK proofs for linear subspaces. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part I. LNCS, vol. 8269, pp. 1–20. Springer, Heidelberg (2013)
16. Kiltz, E., Pietrzak, K., Stam, M., Yung, M.: A new randomness extraction paradigm for hybrid encryption. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 590–609. Springer, Heidelberg (2009)
17. Lewko, A.: Tools for simulating features of composite order bilinear groups in the prime order setting. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 318–335. Springer, Heidelberg (2012)
18. Lewko, A., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully secure functional encryption: Attribute-based encryption and (Hierarchical) inner product encryption. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 62–91. Springer, Heidelberg (2010)
19. Lewko, A., Waters, B.: New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 455–479. Springer, Heidelberg (2010)
20. Lewko, A., Waters, B.: Why proving HIBE systems secure is difficult. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 58–76. Springer, Heidelberg (2014)
21. Naor, M., Reingold, O.: Number-theoretic constructions of efficient pseudo-random functions. In: 38th FOCS, pp. 458–467. IEEE Computer Society Press (October 1997)
22. Naor, M., Reingold, O.: On the construction of pseudo-random permutations: Luby-Rackoff revisited (extended abstract). In: 29th ACM STOC, pp. 189–199. ACM Press (May 1997)
23. Sakai, R., Ohgishi, K., Kasahara, M.: Cryptosystems based on pairing. In: SCIS 2000, Okinawa, Japan (January 2000)
24. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)
25. Waters, B.: Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 619–636. Springer, Heidelberg (2009)
26. Waters, B.: Efficient identity-based encryption without random oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005)
27. Wee, H.: Dual system encryption via predicate encodings. In: Lindell, Y. (ed.) TCC 2014. LNCS, vol. 8349, pp. 616–637. Springer, Heidelberg (2014)