Identity-based Encryption Tightly Secure under Chosen-ciphertext Attacks

Dennis Hofheinz[1], Dingding Jia[2,3,4], and Jiaxin Pan[1]

[1] Karlsruhe Institute of Technology, Karlsruhe, Germany
{Dennis.Hofheinz, Jiaxin.Pan}@kit.edu
[2] State Key Laboratory of Information Security, Institute of Information Engineering, CAS, Beijing, China
jiadingding@iie.ac.cn
[3] Data Assurance and Communication Security Research Center, IIE, CAS, Beijing, China
[4] School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China

Abstract We propose the first identity-based encryption (IBE) scheme that is (almost) tightly secure against chosen-ciphertext attacks. Our scheme is efficient, in the sense that its ciphertext overhead is only seven group elements, three group elements more than that of the state-of-the-art passively (almost) tightly secure IBE scheme. Our scheme is secure in a multi-challenge setting, i.e., in face of an arbitrary number of challenge ciphertexts. The security of our scheme is based upon the standard symmetric external Diffie-Hellman assumption in pairing-friendly groups, but we also consider (less efficient) generalizations under weaker assumptions.

Keywords. identity-based encryption, chosen-ciphertext security, tight security reductions.

1 Introduction

Tight security. Usually, security reductions are used to argue the security of a cryptographic scheme S. A reduction reduces any attack on S to an attack on a suitable computational problem P. More specifically, a reduction constructs a successful P-solver $\mathcal{A}_P$ out of any given successful adversary $\mathcal{A}_S$ on S. Intuitively, a reduction thus shows that S is at least as hard to break/solve as P.

Ideally, we would like a reduction to be *tight*, in the sense that the constructed $\mathcal{A}_P$ has the same complexity and success probability as the given $\mathcal{A}_S$. A tight security reduction implies that the security of S is tightly coupled with the hardness of P. From a more practical perspective, a tight security reduction allows for more efficient parameter choices for S, when deriving those parameters from the best known attacks on P.

Current state of the art. Tight reductions have been studied for a variety of cryptographic primitives, such as public-key encryption [6,29,37,38,27,17,28],

signature schemes [10,13,29,1,12,8,37,27,2,4,43,18,32], identity-based encryption (IBE) [12,8,31,3,21,22,11], non-interactive zero-knowledge proofs [29,37,17], and key exchange [5,26].

Existing tight reductions and corresponding schemes differ in the type and quality of tightness, and in the incurred cost of tightness. For instance, most of the referenced works provide only what is usually called "almost tight" reductions. In an almost tight reduction, the success probability of $\mathcal{A}_P$ may be smaller than $\mathcal{A}_S$, but only by a factor depends only on the security parameter (but not, e.g., on the size of $\mathcal{A}_S$). Furthermore, some reductions consider the scheme only in a somewhat restricted setting, such as an IBE setting in which only one challenge ciphertext is considered.

Our goal: (almost) tightly CCA-secure IBE schemes in the multi-challenge setting. In this work, we are interested in (almost) tight reductions for IBE schemes. As remarked above, there already exist a variety of (almost) tightly secure IBE schemes. However, most of these schemes only provide security of one challenge ciphertext, and none of them provide security against chosen-ciphertext attacks. Security of many challenge ciphertexts is of course a more realistic notion; and while this notion is polynomially equivalent to the one-challenge notion, the corresponding reduction is far from tight, and defeats the purpose of tight security of the overall scheme in a realistic setting. Furthermore, chosen-ciphertext security guarantees security even against active adversaries [42].

On the difficulty of achieving our goal. Achieving many-challenge IBE security and chosen-ciphertext security appears to be technically challenging. First, with the exception of [21,22], all known IBE constructions that achieve (almost) tight many-challenge security rely on composite-order groups, and are thus comparatively inefficient. The exception [22] (like its predecessor [21]) constructs an efficient (almost) tightly secure IBE scheme in the many-challenge setting by adapting and implementing the "(extended) nested dual system groups" framework [12,31] in prime-order groups. Since this work is closest to ours, we will take a closer look at it after we have described our technical contribution. We stress, however, that also [22] does not achieve chosen-ciphertext security.

Second, canonical approaches to obtain chosen-ciphertext security do not appear to apply to existing tightly secure IBE schemes. For instance, it is known that *hierarchical* identity-based encryption (HIBE) implies chosen-ciphertext secure IBE [9]. However, currently no tightly secure HIBE schemes are known, and in fact there are lower bounds on the quality of (a large class of) security reductions for HIBE schemes [36].

Another natural approach to achieve chosen-ciphertext security is to equip ciphertexts with a non-interactive zero-knowledge (NIZK) proof of knowledge of the corresponding plaintext. Intuitively, a security reduction can use this NIZK proof to extract the plaintext message from any adversarially generated decryption query. Highly optimized variants of this outline are responsible for highly efficient public-key encryption schemes (e.g., [41,14,35]).

It is plausible that this approach can be used to turn, e.g., the tightly secure schemes of [21,22] into chosen-ciphertext secure schemes. However, this requires a NIZK proof system which is tightly secure and sound even in the presence of many simulated proofs. While such proof systems are constructible by combining Groth-Sahai proofs [24] with a tightly secure structure-preserving signature scheme [18] (see also [23,29]), the resulting NIZK and IBE schemes would not be very efficient. In fact, efficient suitable NIZK schemes are only known for simple languages [17], which do not appear compatible with the complex IBE schemes of [21,22].

Our results. We provide a tightly chosen-ciphertext secure IBE scheme in the multi-challenge setting. Our scheme builds upon a new tightly chosen-plaintext secure IBE scheme whose efficiency is comparable with that of the state-of-the-art scheme of [22]. However, unlike [22], our scheme *is* compatible with the highly efficient NIZK proof system of [17]. This allows to upgrade our scheme to chosen-ciphertext security by adding an efficient consistency proof (that consists of only three group elements) to ciphertexts. We briefly remark that, similar to previous schemes [8,3,21,22], our scheme also achieves a (somewhat weak) form of anonymity. We compare the efficiency of our scheme with existing state-of-the-art schemes in Table 1.

Scheme	$\lvert\mathsf{pk}\rvert$	$\lvert\mathsf{C}\rvert$	MC	CCA	Loss	Assump.
Gen06 [19]	$5\lvert\mathbb{G}_1\rvert + \lvert\mathsf{H}\rvert$	$\lvert\mathbb{G}\rvert + 2\lvert\mathbb{G}_T\rvert$	–	√	$O(1)$	q-ABDHE
CW13 [12]	$2k^2(2\lambda+1)\lvert\mathbb{G}_1\rvert + k\lvert\mathbb{G}_T\rvert$	$4k\lvert\mathbb{G}_1\rvert$	–	–	$O(\lambda)$	k-LIN
BKP14 [8]	$(2\lambda k^2 + 2k)\lvert\mathbb{G}_1\rvert$	$(2k+1)\lvert\mathbb{G}_1\rvert$	–	–	$O(\lambda)$	k-LIN
AHY15 [3]	$(16\lambda+8)\lvert\mathbb{G}_1\rvert + 2\lvert\mathbb{G}_T\rvert$	$8\lvert\mathbb{G}_1\rvert$	√	–	$O(\lambda)$	k-LIN
GCD$^+$16 [21]	$(6\lambda k^2 + 3k^2)\lvert\mathbb{G}_1\rvert + k\lvert\mathbb{G}_T\rvert$	$6k\lvert\mathbb{G}_1\rvert$	√	–	$O(\lambda)$	k-LIN
GCD$^+$16 [21]	$(4\lambda k^2 + 2k^2)\lvert\mathbb{G}_1\rvert + k\lvert\mathbb{G}_T\rvert$	$4k\lvert\mathbb{G}_1\rvert$	√	–	$O(\lambda)$	k-LINAI
GDCC16 [22]	$(2\lambda k^2 + 3k^2)\lvert\mathbb{G}_1\rvert + k\lvert\mathbb{G}_T\rvert$	$4k\lvert\mathbb{G}_1\rvert$	√	–	$O(\lambda)$	k-LIN
HLQG18 [25]	$(4\lambda k^2 + k^2 + 2k)\lvert\mathbb{G}_1\rvert + \lvert\mathsf{CH}\rvert$	$(2k+1)\lvert\mathbb{G}_1\rvert + \lvert\mathsf{R}\rvert$	–	√	$O(\lambda)$	k-LIN
Ours	$((5+4\lambda)k^2 + (2+2\lambda)k)\lvert\mathbb{G}_1\rvert$ $+(2\lambda k^2 + 4k^2 + k)\lvert\mathbb{G}_2\rvert$	$(6k+1)\lvert\mathbb{G}_1\rvert$	√	√	$O(\lambda)$	k-LIN

Table 1. Comparison between known (almost) tightly and adaptively secure IBEs in prime-order groups from standard assumptions. We count the number of group elements in $\mathbb{G}$ (for symmetric pairings), $\mathbb{G}_1, \mathbb{G}_2$, and $\mathbb{G}_T$. $\lvert\mathsf{pk}\rvert$ denotes the size of the (master) public key, and $\lvert\mathsf{C}\rvert$ denotes the ciphertext overhead (on top of the message size).'MC' denotes many-challenge security, and 'CCA' chosen-ciphertext security. 'Loss' denotes the reduction loss, and 'Assump.' the assumption reduced to. $\mathsf{H} : \mathbb{G} \times \mathbb{G}_T \times \mathbb{G}_T \to \mathbb{Z}_q$ is a universal one-way hash function and $\lvert\mathsf{H}\rvert$ denotes the size of the representation of H. $\lvert\mathsf{CH}\rvert$ is the size of the hash key of a chameleon hash $\mathsf{CH} : \mathbb{G}_1^{k+1} \to \{0,1\}^L$ and $\lvert\mathsf{R}\rvert$ is the size of its randomness.

1.1 Technical overview

The approach of Blazy, Kiltz, and Pan (BKP). Our starting point is the MAC→IBE transformation of Blazy, Kiltz, and Pan (BKP) [8], which in turn abstracts the IBE construction of Chen and Wee [12], and generalizes the

PRF→signatures transformation of Bellare and Goldwasser [7]. The BKP transformation assumes an "affine message authentication code" (affine MAC), i.e., a MAC in which verification consists in checking a system of affine equations. The variables in these affine equations comprise the MAC secret key, and the (public) coefficients are derived from the message to be signed.

This affine MAC is turned into an IBE scheme as follows: the IBE master public key $\mathsf{pk} = \mathsf{Com}(\mathsf{K})$ consists of a commitment to the MAC secret key K. An IBE user secret key $\mathsf{usk}[\mathsf{id}]$ for an identity id consists of a MAC tag τ_{id} on the message id, along with a NIZK proof that τ_{id} indeed verifies correctly relative to pk. The key observation of BKP is now that we can implement commitments and NIZK proof using the Groth-Sahai proof system [24]. Since the used MAC is affine, the corresponding verification involves only linear equations, which makes the corresponding proofs rerandomizable.

Now an IBE ciphertext C essentially contains a rerandomized version of the public, say, left-hand side of the NIZK equations for verifying the validity of τ_{id}. The corresponding right-hand side can be computed either from the randomization information (known to the sender), or using the NIZK proof for τ_{id} (known to the receiver through $\mathsf{usk}[\mathsf{id}]$). Of course, this technique relies on subtleties of the Groth-Sahai proof system that our high-level overview cannot cover.

Advantages and limitations of the BKP approach. The BKP approach has the nice property that the (one-challenge, chosen-plaintext) security of the resulting IBE scheme can be tightly reduced to the (one-challenge) security of the MAC scheme. In particular, BKP also gave a MAC scheme which is tightly secure in a one-challenge setting under a standard computational assumption. At the same time, BKP only consider one IBE challenge ciphertext, and chosen-plaintext security. In particular in large-scale scenarios with huge amounts of ciphertexts and active adversaries, this again defeats the purpose of a tight reduction.

First modification: achieving many-challenge security. We will first show that the BKP reduction can be easily extended to the many-challenge case, assuming of course that the underlying MAC scheme is secure in the many-challenge setting. In this, the actual difficulty lies in constructing a suitable MAC scheme. We do so by adapting the affine MAC $\mathsf{MAC}_{\mathsf{BKP}}$ of BKP, using ideas from the recent (almost) tightly secure PKE scheme of Gay et al. [17].

More specifically, $\mathsf{MAC}_{\mathsf{BKP}}$ operates in a group $\mathbb{G} = \langle g \rangle$ of order q. We use the implicit notation $[x] := g^x$ for group elements. $\mathsf{MAC}_{\mathsf{BKP}}$ assumes a public matrix $[\mathbf{B}] \in \mathbb{G}^{n \times n}$ of a dimension n that depends on the underlying computational assumption. Its secret key is of the form

$$\mathsf{sk}_{\mathsf{MAC}} = ((\mathbf{x}_{i,b})_{i,b}, x'_0) \ \in \ (\mathbb{Z}_q^n)^{\ell \cdot 2} \times \mathbb{Z}_q,$$

and a tag for a message $\mathsf{m} \in \{0,1\}^\ell$ is of the form

$$\tau = ([\mathbf{t}], [u]) \in \mathbb{G}^n \times \mathbb{G} \quad \text{with} \quad \begin{array}{l} \mathbf{t} = \mathbf{B}\mathbf{s} \in \mathbb{Z}_q^n \quad \text{for} \quad \mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^{n'} \\ u = \sum_i \mathbf{x}_{i,\mathsf{m}_i}^\top \mathbf{t} + x'_0 \in \mathbb{Z}_q \end{array}. \tag{1}$$

Verification checks that u is of the form from (1).

We sketch now a bit more specifically how $\mathsf{MAC}_{\mathsf{BKP}}$'s security proof proceeds, assuming an adversary $\mathcal{A}$ in the EUF-CMA security game. The overall strategy is to gradually randomize all u values issued in $\mathcal{A}$'s tag queries. This is equivalent to using different and independent "virtual" secret keys for each message. Hence, once this is done, $\mathcal{A}$ cannot be successful by an information-theoretic argument.

The main difficulty in randomizing all u is that a reduction must be able to still evaluate $\mathcal{A}$'s success in forging a tag for fresh message. In particular, the reduction must be able to compute $u^* = \sum \mathbf{x}_{i,\mathsf{m}_i^*}^\top \mathbf{t}^* + x_0'$ for a message m^* and value $\mathbf{t}^*$ adaptively selected by $\mathcal{A}$. The solution chosen by BKP, following Chen and Wee [12], is to iterate over all bit indices i. For each i, the reduction guesses the i-th bit m_i^* of $\mathcal{A}$'s forgery message, and embeds a computational challenge into $\mathbf{x}_{i,1-\mathsf{m}_i^*}$. This allows to randomize all u in issued tags with $\mathsf{m}_i \neq \mathsf{m}_i^*$, and still be able to evaluate u^*. The corresponding reduction loses a multiplicative factor of only $O(\ell)$. However, note that this strategy would not work with multiple challenges (i.e., potential forgeries (m^*, τ^*)) from $\mathcal{A}$. For instance, the simulation above is always only able to verify a given τ^* for exactly one of the two messages $\mathsf{m}_0^* = 0^\ell$ and $\mathsf{m}_1^* = 1^\ell$.

Our solution here is to instead employ the randomization strategy used by Gay et al. [17] in the context of public-key encryption. Namely, we first increase the dimension of $\mathbf{x}$. This allows us to essentially randomize both tags for messages with $\mathsf{m}_i = 0$ *and* $\mathsf{m}_i = 1$ simultaneously, using different parts of the $\mathbf{x}_{i,b}$ independently. In particular, we will embed computational challenges in different parts of both $\mathbf{x}_{i,0}$ and $\mathbf{x}_{i,1}$. This allows to adapt the argument of Gay et al. to the case of MACs, and hence to prove a slight variant of the BKP MAC secure even under many-challenge attacks.

Second modification: achieving chosen-ciphertext security. So far, we could almost completely follow the BKP approach, with only a slight twist to the BKP MAC, and by adapting the proof strategy of Gay et al. However, the resulting scheme is still not chosen-ciphertext secure. To achieve chosen-ciphertext security, we will follow one of the generic approaches outlined above. In this, the modular structure of the BKP IBE, and the simplicity of the used MAC will pay off.

More concretely, following Naor and Yung [41], we will add a NIZK proof to each ciphertext. Unlike in the generic paradigm of achieving chosen-ciphertext security via NIZK proofs, we do not explicitly prove knowledge of the corresponding plaintext. Instead, following Cramer and Shoup [14], we prove only consistency of the ciphertext, in the sense that the ciphertext is a possible output of the encryption algorithm. Compared to a NIZK proof of knowledge (of plaintext), this yields a much more efficient scheme, but also requires more subtle proof of security.

Our security argument is reminiscent of that of Cramer and Shoup, but of course adapted to the IBE setting. Our reduction will be able to generate user decryption keys for all identities. These decryption keys will function perfectly well on consistent (in the above sense) ciphertexts at all times in the proof, but their action on inconsistent ciphertexts will be gradually randomized. Hence,

adversarial decryption queries, whose consistency is guaranteed by the attached NIZK proof, will be decrypted correctly at all times. On the other hand, all generated challenge ciphertexts will be made inconsistent and will be equipped with simulated NIZK proofs early on.

Unlike Cramer and Shoup, who considered only one challenge ciphertext (for a PKE scheme), we need a very powerful NIZK scheme which enjoys (almost) tight unbounded simulation-soundness. Fortunately, the language for which we require this scheme is linear (due to the restriction to affine MACs), and hence we can use (a slight variant of) the highly efficient NIZK scheme from [17].

We stress that this proof blueprint is compatible with the proof of the BKP transformation, even when adapted to many challenges as explained above. In particular, we are able to extend the BKP transformation not only to many challenges, but also (and additionally) to chosen-ciphertext security. The resulting transformation is black-box and works for any given affine MAC that is secure in a many-challenge setting.

1.2 More on related work

We are not aware of any (almost) tightly chosen-ciphertext secure IBE scheme in the many-challenge setting. A natural idea is of course to adapt existing (almost) tightly chosen-plaintext secure schemes to chosen-ciphertext security. As we have explained in Section 1 above, straightforward generic approaches fail. However, another natural approach is to look at concrete state-of-the-art IBE schemes, and try to use their specific properties. Since we are interested in schemes in prime-order groups for efficiency reasons, the scheme to consider here is that of Gong et al. [22] (cf. also Table 1).

Remark about and comparison to the work of Gong et al. Interestingly, Gong et al. also take the BKP scheme as a basis, and extend it to (chosen-plaintext) many-challenge security, even in a setting with many instances of the IBE scheme itself. However, they first interpret and then extend the BKP scheme in the framework of (extended) nested dual system groups [12,31]. Remarkably, the resulting IBE scheme looks similar to the chosen-plaintext secure, many-challenge scheme that we use as a stepping stone towards many-challenge chosen-ciphertext security. In particular, the efficiency characteristics of those two schemes are comparable.

Still, for the express purpose of achieving chosen-ciphertext security, we found it easier to stick to (an extension of) the original BKP transformation and strategy, for two reasons. First, the modularity of BKP allows us to give an abstract MAC→IBE transformation that achieves chosen-ciphertext security. This allows to isolate the intricate many-challenge security argument for the MAC from the orthogonal argument to achieve chosen-ciphertext security. Since the argument for tight security is directly woven into the notion of (extended) nested dual systems groups, it does not seem clear how to similarly isolate arguments (and proof complexity) for the scheme and strategy of Gong et al.

Second, as hinted above, our strategy to obtain chosen-ciphertext security requires a NIZK proof to show consistency of a ciphertext. With the BKP construction, consistency translates to a statement from a linear language, which allows to employ very efficient NIZK proof systems. For the construction of Gong et al., it is not clear how exactly such a consistency language would look like. In particular, it is not clear at all if highly efficient NIZK proofs for linear languages can be used.[5]

2 Basic preliminaries

2.1 Notations

We use $x \xleftarrow{\$} \mathcal{S}$ to denote the process of sampling an element x from $\mathcal{S}$ uniformly at random if $\mathcal{S}$ is a set. For positive integers $k > 1, \eta \in \mathbb{Z}^+$ and a matrix $\mathbf{A} \in \mathbb{Z}_q^{(k+\eta)\times k}$, we denote the upper square matrix of $\mathbf{A}$ by $\overline{\mathbf{A}} \in \mathbb{Z}_q^{k\times k}$ and the lower η rows of $\mathbf{A}$ by $\underline{\mathbf{A}} \in \mathbb{Z}_q^{\eta\times k}$. Similarly, for a column vector $\mathbf{v} \in \mathbb{Z}_q^{k+\eta}$, we denote the upper k elements by $\overline{\mathbf{v}} \in \mathbb{Z}_q^k$ and the lower η elements of $\mathbf{v}$ by $\underline{\mathbf{v}} \in \mathbb{Z}_q^\eta$. For a bit string $\mathsf{m} \in \{0,1\}^n$, m_i denotes the ith bit of m ($i \leq n$) and $\mathsf{m}_{|i}$ denotes the first i bits of m.

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

Games. We follow [8] to use code-based games for defining and proving security. A game G contains procedures Init and Finalize, and some additional procedures $\mathrm{P}_1, \ldots, \mathrm{P}_n$, which are defined in pseudo-code. Initially all variables in a game are undefined (denoted by $\perp$), and all sets are empty (denote by $\emptyset$). An adversary $\mathcal{A}$ is executed in game G (denote by $\mathsf{G}^{\mathcal{A}}$) if it first calls Init, obtaining its output. Next, it may make arbitrary queries to P_i (according to their specification), again obtaining their output. Finally, it makes one single call to Finalize$(\cdot)$ and stops. We use $\mathsf{G}^{\mathcal{A}} \Rightarrow d$ to denote that G outputs d after interacting with $\mathcal{A}$, and d is the output of Finalize.

2.2 Collision resistant hash functions

Let $\mathcal{H}$ be a family of hash functions $H : \{0,1\}^* \to \{0,1\}^\lambda$. We assume that it is efficient to sample a function from $\mathcal{H}$, which is denoted by $H \xleftarrow{\$} \mathcal{H}$.

Definition 1 (Collision resistance). *We say a family of hash functions $\mathcal{H}$ is (t,ε)-collision-resistant (CR) if for all adversaries $\mathcal{A}$ that run in time t,*

$$\Pr[x \neq x' \wedge H(x) = H(x') \mid H \xleftarrow{\$} \mathcal{H}, (x,x') \xleftarrow{\$} \mathcal{A}(1^\lambda, H)] \leq \varepsilon.$$

[5] To be clear: we do not claim that the scheme of Gong et al. cannot be upgraded to chosen-ciphertext security. However, it seems that such an upgrade would require a more complex restructuring of their proof strategy.

2.3 Pairing groups and matrix Diffie-Hellman assumptions

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

We use implicit representation of group elements as in [16]. For $s \in \{1, 2, T\}$ and $a \in \mathbb{Z}_q$ define $[a]_s = aP_s \in \mathbb{G}_s$ as the implicit representation of a in $\mathbb{G}_s$. Similarly, for a matrix $\mathbf{A} = (a_{ij}) \in \mathbb{Z}_q^{n\times m}$ we define $[\mathbf{A}]_s$ as the implicit representation of $\mathbf{A}$ in $\mathbb{G}_s$. $\mathsf{Span}(\mathbf{A}) := \{\mathbf{Ar} | \mathbf{r} \in \mathbb{Z}_q^m\} \subset \mathbb{Z}_q^n$ denotes the linear span of $\mathbf{A}$, and similarly $\mathsf{Span}([\mathbf{A}]_s) := \{[\mathbf{Ar}]_s | \mathbf{r} \in \mathbb{Z}_q^m\} \subset \mathbb{G}_s^n$. Note that it is efficient to compute $[\mathbf{AB}]_s$ given $([\mathbf{A}]_s, \mathbf{B})$ or $(\mathbf{A}, [\mathbf{B}]_s)$ with matching dimensions. We define $[\mathbf{A}]_1 \circ [\mathbf{B}]_2 := e([\mathbf{A}]_1, [\mathbf{B}]_2) = [\mathbf{AB}]_T$, which can be efficiently computed given $[\mathbf{A}]_1$ and $[\mathbf{B}]_2$.

Next we recall the definition of the matrix Diffie-Hellman (MDDH) and related assumptions [16].

Definition 2 (Matrix distribution). *Let $k, \ell \in \mathbb{N}$ with $\ell > k$. We call $\mathcal{D}_{\ell,k}$ a matrix distribution if it outputs matrices in $\mathbb{Z}_q^{\ell\times k}$ of full rank k in polynomial time. Let $\mathcal{D}_k := \mathcal{D}_{k+1,k}$.*

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

Definition 3 ($\mathcal{D}_{\ell,k}$-Matrix Diffie-Hellman assumption). *Let $\mathcal{D}_{\ell,k}$ be a matrix distribution and $s \in \{1, 2, T\}$. We say that the $\mathcal{D}_{\ell,k}$-Matrix Diffie-Hellman ($\mathcal{D}_{\ell,k}$-MDDH) is (t, ε)-hard relative to GGen in group $\mathbb{G}_s$ if for all adversaries $\mathcal{A}$ with running time t, it holds that*

$$|\Pr[\mathcal{A}(\mathcal{G}, [\mathbf{A}]_s, [\mathbf{Aw}]_s) = 1] - \Pr[\mathcal{A}(\mathcal{G}, [\mathbf{A}]_s, [\mathbf{u}]_s) = 1]| \leq \varepsilon,$$

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

We define the $\mathcal{D}_k$-Kernel Diffie-Hellman ($\mathcal{D}_k$-KerMDH) assumption [39] which is a natural search variant of the $\mathcal{D}_k$-MDDH assumption.

Definition 4 ($\mathcal{D}_k$-Kernel Diffie-Hellman assumption). *Let $\mathcal{D}_k$ be a matrix distribution and $s \in \{1, 2\}$. We say that the $\mathcal{D}_k$-kernel Matrix Diffie-Hellman ($\mathcal{D}_k$-KerMDH) is (t, ε)-hard relative to GGen in group $\mathbb{G}_s$ if for all adversaries $\mathcal{A}$ that runs in time t, it holds that*

$$\Pr[\mathbf{c}^\top \mathbf{A} = \mathbf{0} \wedge \mathbf{c} \neq \mathbf{0} | [\mathbf{c}]_{3-s} \xleftarrow{\$} \mathcal{A}(\mathcal{G}, [\mathbf{A}]_s)] \leq \varepsilon,$$

where the probability is taken over $\mathcal{G} \xleftarrow{\$} \mathsf{GGen}(1^\lambda)$, $\mathbf{A} \xleftarrow{\$} \mathcal{D}_k$.

The following lemma shows that the $\mathcal{D}_k$-KerMDH assumption is a relaxation of the $\mathcal{D}_k$-MDDH assumption since one can use a non-zero vector in the kernel of $\mathbf{A}$ to test membership in the column space of $\mathbf{A}$.

Lemma 1 ($\mathcal{D}_k$-MDDH $\Rightarrow$ $\mathcal{D}_k$-KerMDH [39]). *For any matrix distribution* $\mathcal{D}_k$, *if* $\mathcal{D}_k$-MDDH *is* (t, ε)*-hard in* $\mathbb{G}_s$, *then* $\mathcal{D}_k$-KerMDH *is* (t', ε)*-hard in* $\mathbb{G}_s$, *where* $t' \approx t$.

The uniform distribution is a particular matrix distribution that deserves special attention, as an adversary breaking the $\mathcal{U}_{\ell,k}$ assumption can also distinguish between real MDDH tuples and random tuples for all other possible matrix distributions. For uniform distributions, they stated in [17] that $\mathcal{U}_k$-MDDH and $\mathcal{U}_{\ell,k}$-MDDH assumptions are equivalent.

Definition 5 (Uniform distribution). *Let* $k, \ell \in \mathbb{N}$ *with* $\ell > k$. *We call* $\mathcal{U}_{\ell,k}$ *a uniform distribution if it outputs uniformly random matrices in* $\mathbb{Z}_q^{\ell \times k}$ *of rank* k *in polynomial time.*

Lemma 2 ($\mathcal{D}_{\ell,k}$-MDDH $\Rightarrow$ $\mathcal{U}_{\ell,k}$-MDDH $\Leftrightarrow$ $\mathcal{U}_k$-MDDH [16,17]). *For* $\ell > k$, *let* $\mathcal{D}_{\ell,k}$ *be a matrix distribution, then if* $\mathcal{D}_{\ell,k}$-MDDH *is* (t, ε)*-hard in* $\mathbb{G}_s$, $\mathcal{U}_{\ell,k}$-MDDH *is* (t', ε)*-hard in* $\mathbb{G}_s$, *where* $t' \approx t$. *If* $\mathcal{U}_k$-MDDH *is* (t, ε)*-hard in* $\mathbb{G}_s$, $\mathcal{U}_{\ell,k}$-MDDH *is* (t', ε)*-hard in* $\mathbb{G}_s$, *where* $t' \approx t$, *vice versa.*

For $Q \in \mathbb{N}$, $\mathbf{W} \xleftarrow{\$} \mathbb{Z}_q^{k \times Q}$, $\mathbf{U} \xleftarrow{\$} \mathbb{Z}_q^{\ell \times Q}$, consider the Q-fold $\mathcal{D}_{\ell,k}$-MDDH problem which is distinguishing the distributions $([\mathbf{A}], [\mathbf{AW}])$ and $([\mathbf{A}], [\mathbf{U}])$. That is, the Q-fold $\mathcal{D}_{\ell,k}$-MDDH problem contains Q independent instances of the $\mathcal{D}_{\ell,k}$-MDDH problem (with the same $\mathbf{A}$ but different $\mathbf{w}_i$). The following lemma shows that the two problems are tightly equivalent. The reduction quality is tighter for uniform distribution.

Lemma 3 (Random self-reducibility [16]). *For* $\ell > k$ *and any matrix distribution* $\mathcal{D}_{\ell,k}$, $\mathcal{D}_{\ell,k}$-MDDH *is random self-reducible. In particular, for any* $Q \geq 1$, *if* $\mathcal{D}_{\ell,k}$-MDDH *is* (t, ε)*-hard relative to* GGen *in group* $\mathbb{G}_s$, *then* Q*-fold* $\mathcal{D}_{\ell,k}$-MDDH *is* (t', ε')*-hard relative to* GGen *in group* $\mathbb{G}_s$, *where* $t \approx t' + Q \cdot \mathsf{poly}(\lambda)$, $\varepsilon' \leq (\ell - k)\varepsilon + \frac{1}{q-1}$, *and for* $\mathcal{D}_{\ell,k} = \mathcal{U}_{\ell,k}$, $\varepsilon' \leq \varepsilon + \frac{1}{q-1}$.

3 Affine MACs in the Multi-Challenge Setting

3.1 Definition

We recall the definition of affine MACs from [8] and extend its security requirements of pseudorandomness to the multi-challenge setting.

Definition 6 (Affine MACs). *Let* par *be system parameters which contain a pairing group description* $\mathcal{G} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$ *of prime order* q, *and let* n *be a positive integer,* $\mathsf{MAC} = (\mathsf{Gen}_{\mathsf{MAC}}, \mathsf{Tag}, \mathsf{Ver}_{\mathsf{MAC}})$ *is an affine MAC over* $\mathbb{Z}_q^n$ *if the following conditions hold:*

INIT:	CHAL(m^*): // at most Q_c queries
$\mathsf{sk}_\mathsf{MAC} \xleftarrow{\$} \mathsf{Gen}_\mathsf{MAC}(\mathsf{par})$	$\mathcal{C}_\mathcal{M} = \mathcal{C}_\mathcal{M} \cup \{\mathsf{m}^*\}$
Return ϵ	$\mathbf{h} \xleftarrow{\$} \mathbb{Z}_q^\eta$;
	$\mathbf{h}_0 = \sum f_i(\mathsf{m}^*)\mathbf{X_i}^\top \mathbf{h} \in \mathbb{Z}_q^n$
EVAL(m): // at most Q_e queries	$h_1 = \sum f'_i(\mathsf{m}^*){\mathbf{x}'_i}^\top \mathbf{h} \in \mathbb{Z}_q$
$\mathcal{Q}_\mathcal{M} = \mathcal{Q}_\mathcal{M} \cup \{\mathsf{m}\}$	$\mathbf{h}_0 \xleftarrow{\$} \mathbb{Z}_q^n, \quad h_1 \xleftarrow{\$} \mathbb{Z}_q$
If $(\mathbf{t}_\mathsf{m}, \mathbf{u}_\mathsf{m}) = (\bot, \bot)$ then	Return $([\mathbf{h}]_1, [\mathbf{h}_0]_1, [h_1]_T)$
$([\mathbf{t}_\mathsf{m}]_2, [\mathbf{u}_\mathsf{m}]_2) \xleftarrow{\$} \mathsf{Tag}(\mathsf{sk}_\mathsf{MAC}, \mathsf{m})$	
Return $([\mathbf{t}_\mathsf{m}]_2, [\mathbf{u}_\mathsf{m}]_2)$	FINALIZE($d \in \{0,1\}$):
	Return $d \wedge (\mathcal{Q}_\mathcal{M} \cap \mathcal{C}_\mathcal{M} = \emptyset)$

Figure 1. Games $\mathsf{mPR\text{-}CMA}_0$ and $\mathsf{mPR\text{-}CMA}_1$ for defining mPR-CMA security.

1. $\mathsf{sk}_\mathsf{MAC} \xleftarrow{\$} \mathsf{Gen}_\mathsf{MAC}(\mathsf{par})$, *where* $\mathsf{sk}_\mathsf{MAC} = (\mathbf{B}, \mathbf{X}_0, ..., \mathbf{X}_\ell, \mathbf{x}'_0, ..., \mathbf{x}'_{\ell'}) \in \mathbb{Z}_q^{n \times n'} \times (\mathbb{Z}_q^{\eta \times n})^{\ell+1} \times (\mathbb{Z}_q^\eta)^{\ell'+1}$, *$n', \ell, \ell'$ and η are positive integers and the rank of $\mathbf{B}$ is at least 1.*
2. $\tau \xleftarrow{\$} \mathsf{Tag}(\mathsf{sk}_\mathsf{MAC}, \mathsf{m})$, *where* $\tau := ([\mathbf{t}]_2, [\mathbf{u}]_2) \in \mathbb{G}_2^n \times \mathbb{G}_2^\eta$ *is computed as*

$$\mathbf{t} := \mathbf{B}\mathbf{s} \in \mathbb{Z}_q^n \quad \textit{for} \quad \mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^{n'} \tag{2}$$

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

   for some public defining functions $f_i : \mathcal{M} \to \mathbb{Z}_q$ and $f'_i : \mathcal{M} \to \mathbb{Z}_q$. Note that only $\mathbf{u}$ is the message dependent part.
3. $\mathsf{Ver}_\mathsf{MAC}(\mathsf{sk}_\mathsf{MAC}, \mathsf{m}, \tau = ([\mathbf{t}]_2, [\mathbf{u}]_2))$ *output 1 iff (3) holds, 0 otherwise.*

Definition 7. *An affine* MAC *over $\mathbb{Z}_q^n$ is $(Q_\mathsf{e}, Q_\mathsf{c}, t, \varepsilon)$-*mPR-CMA *(pseudorandom against chosen-message and multi-challenge attacks) if for all $\mathcal{A}$ that runs in time t, makes at most Q_e queries to the evaluation oracle,* EVAL*, and at most Q_c queries to the challenge oracle,* CHAL*, the following holds*

$$|\Pr[\mathsf{mPR\text{-}CMA}_0^\mathcal{A} \Rightarrow 1] - \Pr[\mathsf{mPR\text{-}CMA}_1^\mathcal{A} \Rightarrow 1]| \leq \varepsilon,$$

where experiments $\mathsf{mPR\text{-}CMA}_0$ and $\mathsf{mPR\text{-}CMA}_1$ are defined in Figure 1.

Our notion is a generalization of the PR-CMA security in [8]. In [8] an adversary $\mathcal{A}$ can only query the challenge oracle CHAL at most once, while here $\mathcal{A}$ can ask multiple times.

3.2 Instantiation

We extend the tightly secure affine MAC $\mathsf{MAC}_\mathsf{NR}[\mathcal{D}_k]$ from [8] to the multi-challenge setting. Instead of choosing random vectors $\mathbf{x}_{i,b} \in \mathbb{Z}_q^k$ as the MAC secret keys in the original, here we choose random matrices $\mathbf{X}_{i,b} \in \mathbb{Z}_q^{2k \times k}$ such

that in the security proof we can randomize all the tags and at the same time answer multiple challenge queries in a tight way.

Let $\mathcal{G} := (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$ be an asymmetric pairing group and $\mathsf{par} := \mathcal{G}$. Our affine MAC $\mathsf{MAC}^{\mathsf{mc}}_{\mathsf{NR}} := (\mathsf{Gen}_{\mathsf{MAC}}, \mathsf{Tag}, \mathsf{Ver}_{\mathsf{MAC}})$ for message space $\{0,1\}^L$ is defined as follows.

$\underline{\mathsf{Gen}_{\mathsf{MAC}}(\mathsf{par})}$:	$\underline{\mathsf{Tag}(\mathsf{sk}_{\mathsf{MAC}}, \mathsf{m} \in \{0,1\}^L)}$:	$\underline{\mathsf{Ver}_{\mathsf{MAC}}(\mathsf{sk}_{\mathsf{MAC}}, \tau, \mathsf{m})}$:
$\mathbf{A} \xleftarrow{\$} \mathcal{U}_{2k,k}$	$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^k, \mathbf{t} := \mathbf{B}\mathbf{s} \in \mathbb{Z}_q^k$	Parse $\tau := ([\mathbf{t}]_2, [\mathbf{u}]_2)$
$\mathbf{B} := \overline{\mathbf{A}} \in \mathbb{Z}_q^{k \times k}$	$\mathbf{X}_{\mathsf{m}} := \sum_{i=1}^{L} \mathbf{X}_{i,\mathsf{m}_i}$	$\mathbf{X}_{\mathsf{m}} := \sum_{i=1}^{L} \mathbf{X}_{i,\mathsf{m}_i}$
For $1 \le i \le L$ and $b = 0, 1$:	$\mathbf{u} := \mathbf{X}_{\mathsf{m}}\mathbf{t} + \mathbf{x}' \in \mathbb{Z}_q^{2k}$	If $[\mathbf{u}]_2 = [\mathbf{X}_{\mathsf{m}}\mathbf{t} + \mathbf{x}']_2$ then
$\quad \mathbf{X}_{i,b} \xleftarrow{\$} \mathbb{Z}_q^{2k \times k}$	Return $\tau = ([\mathbf{t}]_2, [\mathbf{u}]_2)$	$\quad$ return 1
$\mathbf{x}' \xleftarrow{\$} \mathbb{Z}_q^{2k}$		Else return 0.
$\mathsf{sk}_{\mathsf{MAC}} := (\mathbf{B}, \mathbf{X}_{1,0}, \ldots, \mathbf{X}_{L,1}, \mathbf{x}')$		
Return $\mathsf{sk}_{\mathsf{MAC}}$		

Our scheme can be present by using any $\mathcal{D}_{2k,k}$ distribution and some of them have compact representation and give more efficient scheme. For simplicity of presentation, we present our scheme based on the $\mathcal{U}_{2k,k}$ distribution.

Theorem 1. *If the* $\mathcal{U}_{2k,k}$-MDDH *problem is* (t_1, ε_1)*-hard in* $\mathbb{G}_1$ *and* (t_2, ε_2)*-hard in* $\mathbb{G}_2$*, the* $\mathcal{U}_{2k}$-MDDH *problem is* (t_3, ε_3)*-hard in* $\mathbb{G}_1$*, then* $\mathsf{MAC}^{\mathsf{mc}}_{\mathsf{NR}}$ *is* $(Q_{\mathsf{e}}, Q_{\mathsf{c}}, t_{\mathcal{A}}, \varepsilon)$-mPR-CMA*-secure with* $t_1 \approx t_2 \approx t_3 \approx t_{\mathcal{A}} + (Q_{\mathsf{e}} + Q_{\mathsf{c}})\mathsf{poly}(\lambda)$*, and* $\varepsilon \le 4L\varepsilon_1 + 3L\varepsilon_2 + 3\varepsilon_3 + 2^{-\Omega(\lambda)}$*, where* $\mathsf{poly}(\lambda)$ *is independent of* $t_{\mathcal{A}}$*.*

Proof. We prove the theorem via a sequence of games as shown in Figure 2.

$\underline{\textsc{Init}}$:	$\underline{\textsc{Eval}(\mathsf{m})}$: // G_0, G_3, $\boxed{\mathsf{G}_{1,i}}$, $\ulcorner\mathsf{G}_2\urcorner$
$\mathbf{A} \xleftarrow{\$} \mathcal{U}_{2k,k}$, $\mathbf{B} := \overline{\mathbf{A}}$	$\mathcal{Q}_{\mathcal{M}} := \mathcal{Q}_{\mathcal{M}} \cup \{\mathsf{m}\}$
For $j = 1, \ldots, L$: $\mathbf{X}_{j,0}, \mathbf{X}_{j,1} \xleftarrow{\$} \mathbb{Z}_q^{2k \times k}$	If $([\mathbf{t}_{\mathsf{m}}]_2, [\mathbf{u}_{\mathsf{m}}]_2) = (\bot, \bot)$ then
$\mathbf{x}' \xleftarrow{\$} \mathbb{Z}_q^{2k}$	$\quad \mathbf{s}_{\mathsf{m}} \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{t}_{\mathsf{m}} := \mathbf{B}\mathbf{s}_{\mathsf{m}}$
Return ϵ	$\quad \mathbf{x}'_{\mathsf{m}} := \mathbf{x}'$
	$\quad \boxed{\mathbf{x}'_{\mathsf{m}} := \mathsf{RF}_i(\mathsf{m}_{\mid i})}$
$\underline{\textsc{Chal}(\mathsf{m}^*)}$: // G_0, $\boxed{\mathsf{G}_{1,i}}$, $\ulcorner\mathsf{G}_2, \mathsf{G}_3\urcorner$	$\quad \ulcorner\mathbf{x}'_{\mathsf{m}} \xleftarrow{\$} \mathbb{Z}_q^{2k}\urcorner$
$\mathcal{C}_{\mathcal{M}} := \mathcal{C}_{\mathcal{M}} \cup \{\mathsf{m}^*\}$; $\mathbf{x}'_{\mathsf{m}^*} := \mathbf{x}'$	$\quad \mathbf{u}_{\mathsf{m}} := \sum_{j=1}^{L} \mathbf{X}_{j,\mathsf{m}_j}\mathbf{t}_{\mathsf{m}} + \mathbf{x}'_{\mathsf{m}}$
$\mathbf{h} \xleftarrow{\$} \mathbb{Z}_q^{2k}$; $\boxed{\mathbf{x}'_{\mathsf{m}^*} := \mathsf{RF}_i(\mathsf{m}^*_{\mid i})}$	Return $([\mathbf{t}_{\mathsf{m}}]_2, [\mathbf{u}_{\mathsf{m}}]_2)$
$\mathbf{h}_0 := (\sum_{j=1}^{L} \mathbf{X}_{j,\mathsf{m}^*_j})^\top \mathbf{h}$; $\ulcorner\mathbf{h}_0 \xleftarrow{\$} \mathbb{Z}_q^k\urcorner$	
$h_1 := \mathbf{x}'^{\top}_{\mathsf{m}^*} \mathbf{h} \in \mathbb{Z}_q$; $\ulcorner h_1 \xleftarrow{\$} \mathbb{Z}_q\urcorner$	$\underline{\textsc{Finalize}(d \in \{0,1\})}$:
Return $([\mathbf{h}]_1, [\mathbf{h}_0]_1, [h_1]_T)$	Return $d \wedge (\mathcal{Q}_{\mathcal{M}} \cap \mathcal{C}_{\mathcal{M}} = \emptyset)$

Figure 2. Games G_0, $\mathsf{G}_{1,i}$ $(0 \le i \le L)$, G_2, G_3 for the proof of Theorem 1. $\mathsf{RF}_i : \{0,1\}^i \to \mathbb{Z}_q^{2k}$ is a random function. Boxed codes are only executed in the games marked in the same box style at the top right of every procedure. Non-boxed codes are always run.

Lemma 4 (G_0 **to** $\mathsf{G}_{1,0}$)**.** $\Pr[\text{mPR-CMA}^{\mathcal{A}}_0 \Rightarrow 1] = \Pr[\mathsf{G}^{\mathcal{A}}_0 \Rightarrow 1] = \Pr[\mathsf{G}^{\mathcal{A}}_{1,0} \Rightarrow 1]$.

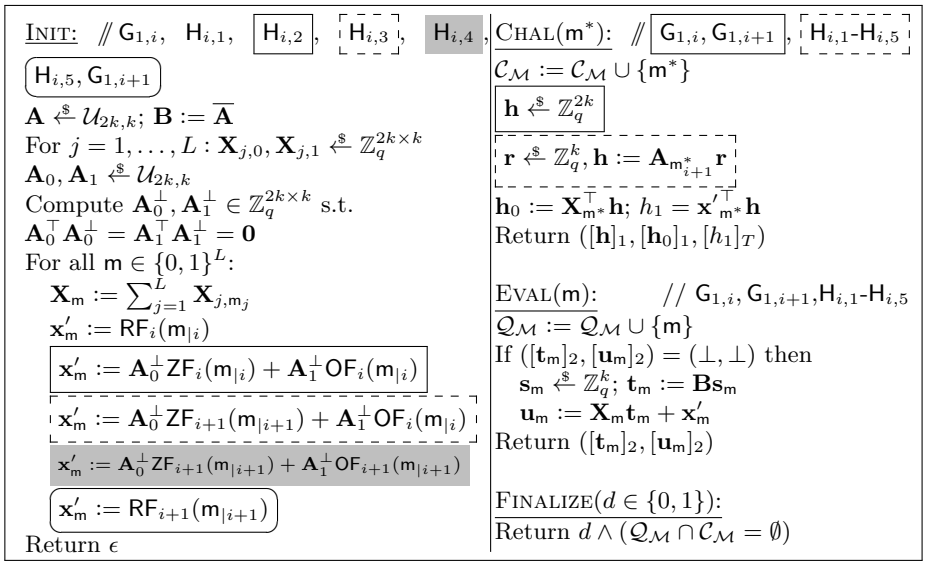

Figure 3. Games $\mathsf{G}_{1,i}$, $\mathsf{G}_{1,i+1}$, $\mathsf{H}_{i,1}$,..., $\mathsf{H}_{i,5}$ $(0 \le i \le L)$ for the proof of Lemma 5. $\mathsf{RF}_i : \{0,1\}^i \to \mathbb{Z}_q^{2k}$, $\mathsf{ZF}_i, \mathsf{OF}_i : \{0,1\}^i \to \mathbb{Z}_q^k$ are three independent random functions.

Proof. G_0 is the original game and it is the same as $\mathsf{mPR\text{-}CMA}_0$. In $\mathsf{G}_{1,0}$, we define $\mathsf{RF}_0(\epsilon)$ as a fix random vector $\mathbf{x}' \xleftarrow{\$} \mathbb{Z}_q^{2k}$ and then have Lemma 4. □

Lemma 5 ($\mathsf{G}_{1,i}$ to $\mathsf{G}_{1,i+1}$). *If the $\mathcal{U}_{2k,k}$-MDDH problem is (t_1, ε_1)-hard in $\mathbb{G}_1$ and (t_2, ε_2)-hard in $\mathbb{G}_2$, then $|\Pr[\mathsf{G}^\mathcal{A}_{1,i} \Rightarrow 1] - \Pr[\mathsf{G}^\mathcal{A}_{1,i+1} \Rightarrow 1]| \le 4\varepsilon_1 + 2\varepsilon_2 + 2^{-\Omega(\lambda)}$ and $t_1 \approx t_2 \approx t_\mathcal{A} + (Q_\mathsf{e} + Q_\mathsf{c})\mathsf{poly}(\lambda)$, where $\mathsf{poly}(\lambda)$ is independent of $t_\mathcal{A}$.*

Proof (of Lemma 5). To bound the difference between $\mathsf{G}_{1,i}$ and $\mathsf{G}_{1,i+1}$, we introduce a series of intermediate games $\mathsf{H}_{i,1}$ to $\mathsf{H}_{i,5}$ as in Figure 3. An overview of the transitions is given in Figure 4.

#	$\mathbf{h}$ in CHAL	$\mathbf{x}'_\mathsf{m}$ in CHAL and EVAL	game knows	remark
$\mathsf{G}_{1,i}$	random	$\mathsf{RF}_i(\mathsf{m}_{\|i})$	-	-
$\mathsf{H}_{i,1}$	$\mathbf{A}_{\mathsf{m}^*_{i+1}}\mathbf{r}$	$\mathsf{RF}_i(\mathsf{m}_{\|i})$	-	$\mathcal{U}_{2k,k}$-MDDH in $\mathbb{G}_1$
$\mathsf{H}_{i,2}$	$\mathbf{A}_{\mathsf{m}^*_{i+1}}\mathbf{r}$	$\mathbf{A}_0^\perp \mathsf{ZF}_i(\mathsf{m}_{\|i}) + \mathbf{A}_1^\perp \mathsf{OF}_i(\mathsf{m}_{\|i})$	$\mathbf{A}_0^\perp, \mathbf{A}_1^\perp$	-
$\mathsf{H}_{i,3}$	$\mathbf{A}_{\mathsf{m}^*_{i+1}}\mathbf{r}$	$\mathbf{A}_0^\perp \mathsf{ZF}_{i+1}(\mathsf{m}_{\|i+1}) + \mathbf{A}_1^\perp \mathsf{OF}_i(\mathsf{m}_{\|i})$	$\mathbf{A}_0^\perp, \mathbf{A}_1^\perp$	$\mathcal{U}_{2k,k}$-MDDH in $\mathbb{G}_2$
$\mathsf{H}_{i,4}$	$\mathbf{A}_{\mathsf{m}^*_{i+1}}\mathbf{r}$	$\mathbf{A}_0^\perp \mathsf{ZF}_{i+1}(\mathsf{m}_{\|i+1}) + \mathbf{A}_1^\perp \mathsf{OF}_{i+1}(\mathsf{m}_{\|i+1})$	$\mathbf{A}_0^\perp, \mathbf{A}_1^\perp$	$\mathcal{U}_{2k,k}$-MDDH in $\mathbb{G}_2$
$\mathsf{H}_{i,5}$	$\mathbf{A}_{\mathsf{m}^*_{i+1}}\mathbf{r}$	$\mathsf{RF}_{i+1}(\mathsf{m}_{\|i+1})$	$\mathbf{A}_0^\perp, \mathbf{A}_1^\perp$	-
$\mathsf{G}_{1,i+1}$	random	$\mathsf{RF}_{i+1}(\mathsf{m}_{\|i+1})$	-	$\mathcal{U}_{2k,k}$-MDDH in $\mathbb{G}_1$

Figure 4. Overview of the transitions in the proof of Lemma 5. We highlight the respective changes between the games in gray. $\mathsf{RF}_i : \{0,1\}^i \to \mathbb{Z}_q^{2k}$, and $\mathsf{ZF}_i, \mathsf{OF}_i : \{0,1\}^i \to \mathbb{Z}_q^k$ are three independent random functions.

Lemma 6 ($\mathsf{G}_{1,i}$ **to** $\mathsf{H}_{i,1}$)**.** *If the* $\mathcal{U}_{2k,k}$-MDDH *problem is* (t_1, ε_1)*-hard in* $\mathbb{G}_1$*, then* $|\Pr[\mathsf{G}^{\mathcal{A}}_{1,i} \Rightarrow 1] - \Pr[\mathsf{H}^{\mathcal{A}}_{i,1} \Rightarrow 1]| \leq 2\varepsilon_1 + 2/(q-1)$ *and* $t_1 \approx t_{\mathcal{A}} + (Q_{\mathsf{e}} + Q_{\mathsf{c}})\mathsf{poly}(\lambda)$*, where* $\mathsf{poly}(\lambda)$ *is independent of* $t_{\mathcal{A}}$*.*

Proof. Let $\mathbf{A}_0, \mathbf{A}_1 \xleftarrow{\$} \mathcal{U}_{2k,k}$. We define an intermediate game $\mathsf{H}'_{i,1}$ which is the same as $\mathsf{G}_{1,i}$ except for CHAL: precisely, if $\mathsf{m}^*_{i+1} = 0$ then we pick $\mathbf{h}$ uniformly random from $\mathsf{Span}(\mathbf{A}_0)$; otherwise, $\mathbf{h} \xleftarrow{\$} \mathbb{Z}_q^{2k}$. Oracles INIT, EVAL and FINALIZE are simulated as in $\mathsf{G}_{1,i}$.

The difference between $\mathsf{G}_{1,i}$ and $\mathsf{H}'_{i,1}$ is bounded by a straightforward reduction to break the Q_{c}-fold $\mathcal{U}_{2k,k}$-MDDH problem in $\mathbb{G}_1$ with $[\mathbf{A}_0]_1$ as the challenge matrix. Thus, by Lemma 3 we have

$$|\Pr[\mathsf{G}^{\mathcal{A}}_{1,i} \Rightarrow 1] - \Pr[\mathsf{H}'^{\mathcal{A}}_{i,1} \Rightarrow 1]| \leq \varepsilon_1 + \frac{1}{q-1}.$$

Similarly, we can bound $\mathsf{H}'_{i,1}$ and $\mathsf{H}_{i,1}$ with the $\mathcal{U}_{2k,k}$-MDDH assumption in $\mathbb{G}_1$, namely,

$$|\Pr[\mathsf{H}'^{\mathcal{A}}_{i,1} \Rightarrow 1] - \Pr[\mathsf{H}^{\mathcal{A}}_{i,1} \Rightarrow 1]| \leq \varepsilon_1 + \frac{1}{q-1}.$$

Here we have $t_1 \approx t_{\mathcal{A}} + (Q_{\mathsf{e}} + Q_{\mathsf{c}})\mathsf{poly}(\lambda)$, where $\mathsf{poly}(\lambda)$ is independent of $t_{\mathcal{A}}$. □

After switching $[\mathbf{h}]_1$ in CHAL to the right span, the following reductions can have $\mathbf{A}_0$ and $\mathbf{A}_1$ over $\mathbb{Z}_q$. Since the rank of $\mathbf{A}_0$ and that of $\mathbf{A}_1$ are both k, we can efficiently compute the kernel matrix $\mathbf{A}_0^{\perp} \in \mathbb{Z}_q^{2k \times k}$ (resp. $\mathbf{A}_1^{\perp}$) of $\mathbf{A}_0$ (resp. $\mathbf{A}_1$). We note that $\mathbf{A}_0^{\top}\mathbf{A}_0^{\perp} = \mathbf{0} = \mathbf{A}_1^{\top}\mathbf{A}_1^{\perp}$ and $(\mathbf{A}_0^{\perp} \mid \mathbf{A}_1^{\perp}) \in \mathbb{Z}_q^{2k \times 2k}$ is a full-rank matrix with overwhelming probability $1 - 2^{-\Omega(\lambda)}$, since $\mathbf{A}_0$ and $\mathbf{A}_1$ are two random matrices.

Let ZF_i and OF_i be two independent random functions mapping from $\{0,1\}^i$ to $\mathbb{Z}_q^k$.

Lemma 7 ($\mathsf{H}_{i,1}$ **to** $\mathsf{H}_{i,2}$)**.** $|\Pr[\mathsf{H}^{\mathcal{A}}_{i,1} \Rightarrow 1] - \Pr[\mathsf{H}^{\mathcal{A}}_{i,2} \Rightarrow 1]| \leq 2^{-\Omega(\lambda)}$.

Proof. The difference between these two games is statistically bounded. In $\mathsf{H}_{i,2}$, we just rewrite $\mathsf{RF}_i(\mathsf{m}_{|i})$ as

$$\mathsf{RF}_i(\mathsf{m}_{|i}) := (\mathbf{A}_0^{\perp} \mid \mathbf{A}_1^{\perp}) \begin{pmatrix} \mathsf{ZF}_i(\mathsf{m}_{|i}) \\ \mathsf{OF}_i(\mathsf{m}_{|i}) \end{pmatrix} \tag{4}$$

Since $(\mathbf{A}_0^{\perp} \mid \mathbf{A}_1^{\perp})$ is a full-rank matrix with overwhelming probability $1 - \frac{k}{q}$ and ZF_i, $\mathsf{OF}_i : \{0,1\}^i \to \mathbb{Z}_q^k$ are two independent random functions, $\mathsf{RF}_i : \{0,1\}^i \to \mathbb{Z}_q^{2k}$ in (4) is a random function as well. Thus, $\mathsf{H}_{i,1}$ and $\mathsf{H}_{i,2}$ are distributed the same except with probability $2^{-\Omega(\lambda)}$. □

The following step is a main difference to $\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k]$ in the original BKP framework [8]. Here our reduction can randomize EVAL queries with the MDDH assumption and at the same time it can answer multiple CHAL queries, while the original $\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k]$ can not. Precisely, to be able to go from RF_i to RF_{i+1}, the security reduction of $\mathsf{MAC}_{\mathsf{NR}}[\mathcal{D}_k]$ (cf. Lemma 3.6 in [8]) guesses $b \xleftarrow{\$} \{0,1\}$ which stands for the $(i+1)$-th bit of m^* and implicitly embeds $\mathbf{T}_{\mathbf{D}} := \underline{\mathbf{D}}\overline{\mathbf{D}}^{-1}$ in the

secret key $\mathbf{x}_{i+1,1-b}$. Note that the reduction does not know $\mathbf{x}_{i+1,1-b}$, but, since the adversary $\mathcal{A}$ only has at most *one* query to CHAL and b is hidden from $\mathcal{A}$, the reduction can hope $\mathsf{m}^*_{i+1} \neq 1-b$ (with probability $1/2$) and it can simulate the experiment. However, this proof strategy does not work in the multi-challenge setting, since $\mathcal{A}$ can ask two challenge queries with one query which has b in the $(i+1)$-th position and $1-b$ in the other.

By increasing the dimension of $\mathbf{X}_{j,\beta}$, our strategy is first embedding $\mathbf{A}_0^\perp \mathbf{T_D}$ in $\mathbf{X}_{i+1,0}$ such that we can add entropy to $\mathbf{x}'_{\mathsf{m}}$ in the span of $\mathbf{A}_0^\perp$ and at the same time upon CHAL queries with 0 in the $(i+1)$-th position $\mathbf{T_D}$ will be canceled out, and then add entropy to $\mathbf{x}'_{\mathsf{m}}$ in the span of $\mathbf{A}_1^\perp$ in the similar way.

Lemma 8 ($\mathsf{H}_{i,2}$ to $\mathsf{H}_{i,3}$). *If the $\mathcal{U}_{2k,k}$-MDDH problem is (t_2, ε_2)-hard in $\mathbb{G}_2$, then $|\Pr[\mathsf{H}^{\mathcal{A}}_{i,2} \Rightarrow 1] - \Pr[\mathsf{H}^{\mathcal{A}}_{i,3} \Rightarrow 1]| \leq \varepsilon_2 + 2^{-\Omega(\lambda)}$ and $t_2 \approx t_{\mathcal{A}} + (Q_{\mathsf{e}} + Q_{\mathsf{c}})\mathsf{poly}(\lambda)$, where $\mathsf{poly}(\lambda)$ is independent of $t_{\mathcal{A}}$.*

Proof. We bound the difference between $\mathsf{H}_{i,2}$ and $\mathsf{H}_{i,3}$ by the Q_{e}-fold $\mathcal{U}_{2k,k}$-MDDH assumption in $\mathbb{G}_2$. Formally, on receiving a Q_{e}-fold $\mathcal{U}_{2k,k}$-MDDH challenge $([\mathbf{D}]_2, [\mathbf{F}]_2 := ([\mathbf{f}_1, \cdots, \mathbf{f}_{Q_{\mathsf{e}}}]_2)) \in \mathbb{G}_2^{2k\times k} \times \mathbb{G}_2^{2k\times Q_{\mathsf{e}}}$, where Q_{e} denotes the number of evaluation queries, we construct a reduction $\mathcal{B}_2$ as in Figure 5. Let $\mathsf{ZF}_i, \mathsf{ZF}'_i$ be two independent random functions, we define ZF_{i+1} as

$$\mathsf{ZF}_{i+1}(\mathsf{m}_{|i+1}) := \begin{cases} \mathsf{ZF}_i(\mathsf{m}_{|i}) + \mathsf{ZF}'_i(\mathsf{m}_{|i}) & \text{if } \mathsf{m}_{i+1} = 0 \\ \mathsf{ZF}_i(\mathsf{m}_{|i}) & \text{if } \mathsf{m}_{i+1} = 1 \end{cases}$$

Note that ZF_{i+1} is a random function, given ZF_i and ZF'_i are two independent random functions. If an adversary $\mathcal{A}$ queries messages m with $\mathsf{m}_{i+1} = 1$ to EVAL and CHAL, then $\mathcal{A}$'s view in $\mathsf{H}_{i,2}$ is the same as that in $\mathsf{H}_{i,3}$. Thus, we only focus on messages with $\mathsf{m}_{i+1} = 0$.

For queries with CHAL, if $\mathsf{m}^*_{i+1} = 0$, $\mathcal{B}_2$ does not have $\mathbf{X}_{i+1,0} = \hat{\mathbf{X}} + \mathbf{A}_0^\perp \underline{\mathbf{D}} \overline{\mathbf{D}}^{-1}$, since $\mathcal{B}_2$ does not know $\underline{\mathbf{D}}\overline{\mathbf{D}}^{-1}$ either over $\mathbb{Z}_q$ or $\mathbb{G}_2$, but, since $\mathbf{h} \in \mathsf{Span}(\mathbf{A}_0)$ for such m^*, $(\mathbf{A}_0^\perp \underline{\mathbf{D}}\overline{\mathbf{D}}^{-1})^\top \mathbf{h} = \mathbf{0}$ and thus $\mathcal{B}_2$ computes

$$\mathbf{h}_0 = (\mathbf{X}_{\mathsf{m}\setminus i+1} + \hat{\mathbf{X}} + \mathbf{A}_0^\perp \underline{\mathbf{D}}\overline{\mathbf{D}}^{-1})^\top \mathbf{h} = (\mathbf{X}_{\mathsf{m}\setminus i+1} + \hat{\mathbf{X}})^\top \mathbf{h}.$$

For queries with EVAL, if $\mathsf{m}_{i+1} = 0$, we write $\mathbf{f}_c := \begin{pmatrix} \overline{\mathbf{D}}\mathbf{w}_c \\ \underline{\mathbf{D}}\mathbf{w}_c + \mathbf{r}_c \end{pmatrix}$ for some $\mathbf{w}_c \in \mathbb{Z}_q^k$, where $\mathbf{r}_c \in \mathbb{Z}_q^k$ is $\mathbf{0}$ if $[\mathbf{F}]_2$ is from the real $\mathcal{U}_{2k,k}$-MDDH distribution, or

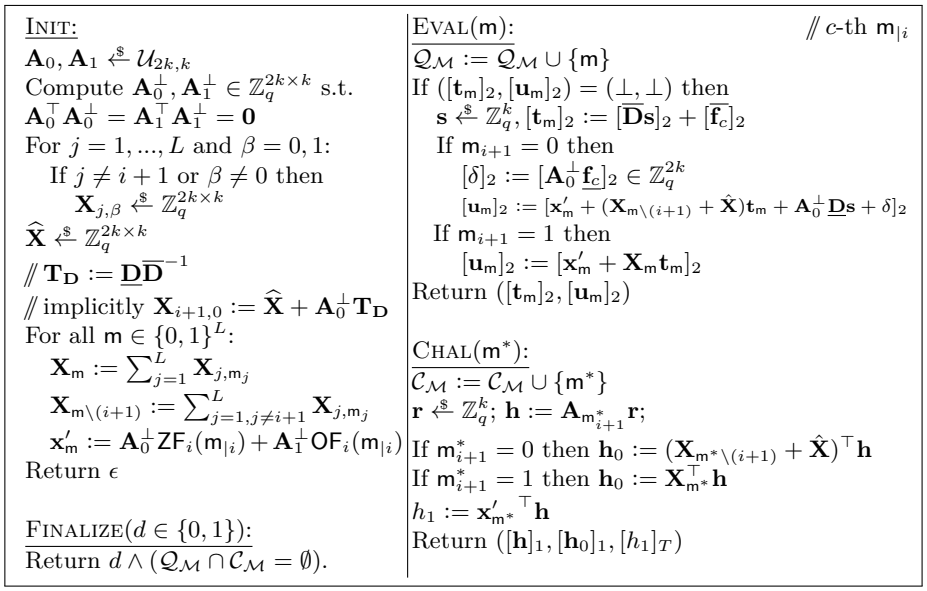

Figure 5. Description of $\mathcal{B}_2(\mathsf{par}, ([\mathbf{D}]_2, [\mathbf{F}]_2))$ for proving Lemma 8.

$\mathbf{r}_c$ is random otherwise. Then, we have

$$\begin{aligned}
\mathbf{u}_\mathsf{m} &:= \mathbf{x}'_\mathsf{m} + \mathbf{X}_{\mathsf{m}\setminus(i+1)}\mathbf{t}_\mathsf{m} + \hat{\mathbf{X}}\mathbf{t}_\mathsf{m} + \mathbf{A}_0^\perp \underline{\mathbf{D}}\mathbf{s} + \mathbf{A}_0^\perp \underline{\mathbf{f}}_c \\
&= \mathbf{x}'_\mathsf{m} + \mathbf{X}_{\mathsf{m}\setminus(i+1)}\mathbf{t}_\mathsf{m} + \hat{\mathbf{X}}\mathbf{t}_\mathsf{m} + \mathbf{A}_0^\perp \underline{\mathbf{D}}\mathbf{s} + \mathbf{A}_0^\perp (\underline{\mathbf{D}}\mathbf{w}_c + \mathbf{r}_c) \\
&= \mathbf{x}'_\mathsf{m} + \mathbf{X}_{\mathsf{m}\setminus(i+1)}\mathbf{t}_\mathsf{m} + \hat{\mathbf{X}}\mathbf{t}_\mathsf{m} + \mathbf{A}_0^\perp \underline{\mathbf{D}}(\mathbf{s} + \mathbf{w}_c) + \mathbf{A}_0^\perp \mathbf{r}_c \\
&= \mathbf{x}'_\mathsf{m} + \mathbf{X}_{\mathsf{m}\setminus(i+1)}\mathbf{t}_\mathsf{m} + \hat{\mathbf{X}}\mathbf{t}_\mathsf{m} + \mathbf{A}_0^\perp \underline{\mathbf{D}}\overline{\mathbf{D}}^{-1} \underbrace{\overline{\mathbf{D}}(\mathbf{s} + \mathbf{w}_c)}_{\mathbf{t}_\mathsf{m}} + \mathbf{A}_0^\perp \mathbf{r}_c \\
&= \mathbf{X}_\mathsf{m}\mathbf{t}_\mathsf{m} + \underbrace{\mathbf{A}_1^\perp \mathsf{OF}_i(\mathsf{m}_{|i}) + \mathbf{A}_0^\perp \mathsf{ZF}_i(\mathsf{m}_{|i})}_{\mathbf{x}'_\mathsf{m}} + \mathbf{A}_0^\perp \mathbf{r}_c
\end{aligned}$$

Now it is clear that if $\mathbf{r}_c = \mathbf{0}$ then $\mathbf{u}_\mathsf{m}$ is distributed as in $\mathsf{H}_{i,2}$; if $\mathbf{r}_c$ is random, then we define $\mathsf{ZF}'_i(\mathsf{m}_{|i}) := \mathbf{r}_c$ and $\mathbf{u}_\mathsf{m}$ is distributed as in $\mathsf{H}_{i,3}$. □

The proof of Lemma 9 is very similar to that of Lemma 8 except that it handles cases with $\mathsf{m}_{i+1} = 1$. More precisely, we define

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

where $\mathsf{OF}_i, \mathsf{OF}'_i$ are two independent random functions mapping from $\{0,1\}^i$ to $\mathbb{Z}_q^k$. By the similar arguments of Lemma 8, we have the following lemma.

Lemma 9 ($\mathsf{H}_{i,3}$ to $\mathsf{H}_{i,4}$). *If the $\mathcal{U}_{2k,k}$-MDDH problem is (t_2, ε_2)-hard in $\mathbb{G}_2$, then $|\Pr[\mathsf{H}^\mathcal{A}_{i,3} \Rightarrow 1] - \Pr[\mathsf{H}^\mathcal{A}_{i,4} \Rightarrow 1]| \leq \varepsilon_2 + 2^{-\Omega(\lambda)}$ and $t_2 \approx t_\mathcal{A}$.*

Lemmata 10 and 11 are the reverse of Lemmata 6 and 7, and we omit the detailed proofs.

Lemma 10 ($\mathsf{H}_{i,4}$ **to** $\mathsf{H}_{i,5}$)**.** $|\Pr[\mathsf{H}^{\mathcal{A}}_{i,4} \Rightarrow 1] - \Pr[\mathsf{H}^{\mathcal{A}}_{i,5} \Rightarrow 1]| \leq 2^{-\Omega(\lambda)}$.

Lemma 11 ($\mathsf{H}_{i,5}$ **to** $\mathsf{G}_{1,i+1}$)**.** *If the* $\mathcal{U}_{2k,k}$-MDDH *problem is* (t_1, ε_1)*-hard in* $\mathbb{G}_1$*, then* $|\Pr[\mathsf{H}^{\mathcal{A}}_{i,5} \Rightarrow 1] - \Pr[\mathsf{G}^{\mathcal{A}}_{1,i+1} \Rightarrow 1]| \leq 2\varepsilon_1 + 2^{-\Omega(\lambda)}$ *and* $t_2 \approx t_{\mathcal{A}} + (Q_{\mathsf{e}} + Q_{\mathsf{c}})\mathsf{poly}(\lambda)$*, where* $\mathsf{poly}(\lambda)$ *is independent of* $t_{\mathcal{A}}$.

Lemma 12 ($\mathsf{G}_{1,L}$ **to** G_2)**.** *If the* $\mathcal{U}_{2k}$-MDDH *problem is* (t_3, ε_3)*-hard in* $\mathbb{G}_1$*, then*

$$|\Pr[\mathsf{G}^{\mathcal{A}}_{1,L} \Rightarrow 1] - \Pr[\mathsf{G}^{\mathcal{A}}_{2} \Rightarrow 1]| \leq 3\varepsilon_3 + 2^{-\Omega(\lambda)} \text{ and } t_3 \approx t_{\mathcal{A}} + (Q_{\mathsf{e}} + Q_{\mathsf{c}})\mathsf{poly}(\lambda),$$

where $\mathsf{poly}(\lambda)$ *is independent of* $t_{\mathcal{A}}$.

Proof. Firstly we bound the difference between $\mathsf{G}_{1,L}$ and $\mathsf{G}_{2'}$ by the Q_{c}-fold $\mathcal{U}_{2k}$-MDDH assumption in $\mathbb{G}_1$, where G'_2 is the same as $\mathsf{G}_{1,L}$ except that on a challenge query, we pick a random $h_1 \xleftarrow{\$} \mathbb{Z}_q$ for each query in G'_2.

Formally, on receiving a Q_{c}-fold $\mathcal{U}_{2k}$-MDDH challenge $([\mathbf{D}]_1, [\mathbf{F}]_1 := ([\mathbf{f}_1, \cdots, \mathbf{f}_{Q_{\mathsf{c}}}]_1)) \in \mathbb{G}_1^{(2k+1)\times 2k} \times \mathbb{G}_1^{(2k+1)\times Q_{\mathsf{c}}}$, where Q_{c} denotes the number of challenge queries, we construct a reduction $\mathcal{B}_2$ as in Figure 6.

INIT:	CHAL(m^*): // c-th query
$\mathbf{A} \xleftarrow{\$} \mathcal{U}_{2k,k}$; $\mathbf{B} := \overline{\mathbf{A}}$	$\mathcal{C}_{\mathcal{M}} := \mathcal{C}_{\mathcal{M}} \cup \{\mathsf{m}^*\}$
For $(j, \beta) \in ([L], \{0,1\})$:	If $\mathsf{RF}'(\mathsf{m}^*) = \perp$, then
$\quad \mathbf{X}_{j,\beta} \xleftarrow{\$} \mathbb{Z}_q^{2k\times k}$	$\quad \mathsf{RF}'(\mathsf{m}^*) \xleftarrow{\$} \mathbb{Z}_q^{2k}$
For all $\mathsf{m} \in \{0,1\}^L$:	$\quad \mathcal{RL} := \mathcal{RL} \cup \{(\mathsf{m}^*, \mathsf{RF}'(\mathsf{m}^*))\}$
$\quad \mathbf{X}_{\mathsf{m}} := \sum_{j=1}^{L} \mathbf{X}_{j,\mathsf{m}_j}$	$[\mathbf{h}]_1 := [\overline{\mathbf{f}_c}]_1$; $[\mathbf{h}_0]_1 := [\mathbf{X}^\top_{\mathsf{m}^*}\mathbf{h}]_1$;
Return ϵ	$[h_1]_1 := [\mathsf{RF}'(\mathsf{m}^*)^\top \overline{\mathbf{f}_c} + \underline{\mathbf{f}_c}]_1$;
	// implicitly set $\mathsf{RF}(\mathsf{m}^*) := \mathsf{RF}'(\mathsf{m}^*) + (\underline{\mathbf{D}}\overline{\mathbf{D}}^{-1})^\top$
EVAL(m):	Return $([\mathbf{h}]_1, [\mathbf{h}_0]_1, [h_1]_T)$
$\mathcal{Q}_{\mathcal{M}} := \mathcal{Q}_{\mathcal{M}} \cup \{\mathsf{m}\}$	
If $([\mathbf{t}_{\mathsf{m}}]_2, [\mathbf{u}_{\mathsf{m}}]_2) = (\perp, \perp)$ then	FINALIZE($d \in \{0,1\}$):
$\quad \mathbf{t}_{\mathsf{m}} \xleftarrow{\$} \mathbb{Z}_q^k$; $\mathbf{u}_{\mathsf{m}} \xleftarrow{\$} \mathbb{Z}_q^{2k}$	Return $d \wedge (\mathcal{Q}_{\mathcal{M}} \cap \mathcal{C}_{\mathcal{M}} = \emptyset)$.
Return $([\mathbf{t}_{\mathsf{m}}]_2, [\mathbf{u}_{\mathsf{m}}]_2)$	

Figure 6. Description of $\mathcal{B}'(\mathcal{G}_1, ([\mathbf{D}]_1, [\mathbf{F}]_1)$ interpolating between G'_2 and $\mathsf{G}_{1,L}$.

For EVAL queries, since $\mathbf{u}_{\mathsf{m}}$ is information-theoretically hidden by $\mathsf{RF}(\mathsf{m})$, we can just pick $\mathbf{u}_{\mathsf{m}}$ uniformly random. For CHAL queries, we write $\mathbf{f}_c := \begin{pmatrix} \overline{\mathbf{D}}\mathbf{w}_c \\ \underline{\mathbf{D}}\mathbf{w}_c + r_c \end{pmatrix}$ for some $\mathbf{w}_c \in \mathbb{Z}_q^{2k}$, where $r_c \in \mathbb{Z}_q$ is 0 if $[\mathbf{F}]_2$ is from the real $\mathcal{U}_{2k}$-MDDH distribution, and r_c is random otherwise. Then, we have

$$\begin{aligned} h_1 &:= \mathsf{RF}'(\mathsf{m}^*)^\top \overline{\mathbf{f}_c} + \underline{\mathbf{f}_c} = \mathsf{RF}'(\mathsf{m}^*)^\top \overline{\mathbf{f}_c} + \underline{\mathbf{D}}\mathbf{w}_c + r_c \\ &= \mathsf{RF}'(\mathsf{m}^*)^\top \overline{\mathbf{f}_c} + \underline{\mathbf{D}}\overline{\mathbf{D}}^{-1}\overline{\mathbf{f}_c} + r_c = \underbrace{(\mathsf{RF}'(\mathsf{m}^*)^\top + \underline{\mathbf{D}}\overline{\mathbf{D}}^{-1})}_{\mathsf{RF}(\mathsf{m}^*)^\top}\overline{\mathbf{f}_c} + r_c. \end{aligned}$$

INIT:	CHAL(m^*): // c-th query
for $(j,\beta) \neq (1,0)$:	$\mathcal{C}_{\mathcal{M}} := \mathcal{C}_{\mathcal{M}} \cup \{\mathsf{m}^*\}$;
$\mathbf{X}_{j,\beta} \xleftarrow{\$} \mathbb{Z}_q^{2k\times k}$	$[\mathbf{h}]_1 := [\overline{\mathbf{f}_c}]_1$;
For all $\mathsf{m} \in \{0,1\}^L$:	If $\mathsf{m}_1^* = 1$ then $[\mathbf{h}_0]_1 := [\mathbf{X}_{\mathsf{m}^*}^\top \mathbf{h}]_1$
$\mathbf{X}_{\mathsf{m}} := \sum_{j=1}^{m} \mathbf{X}_{j,\mathsf{m}_j}$	If $\mathsf{m}_1^* = 0$ then $[\mathbf{h}_0]_1 := [\mathbf{X}_{\mathsf{m}^*\backslash 1}^\top \mathbf{h}]_1 + [\underline{\mathbf{f}_c}]_1$;
$\mathbf{X}_{\mathsf{m}\backslash 1} := \sum_{j=2}^{m} \mathbf{X}_{j,\mathsf{m}_j}$	$h_1 \xleftarrow{\$} \mathbb{Z}_q$;
Return ϵ	// here we implicitly set $\mathbf{X}_{1,0} := (\underline{\mathbf{D}}\overline{\mathbf{D}}^{-1})^\top$;
	Return $([\mathbf{h}]_1, [\mathbf{h}_0]_1, [h_1]_T)$
EVAL(m):	
$\mathcal{Q}_{\mathcal{M}} := \mathcal{Q}_{\mathcal{M}} \cup \{\mathsf{m}\}$	FINALIZE($d \in \{0,1\}$):
If $([\mathbf{t}_{\mathsf{m}}]_2, [\mathbf{u}_{\mathsf{m}}]_2) = (\perp, \perp)$ then	Return $d \wedge (\mathcal{Q}_{\mathcal{M}} \cap \mathcal{C}_{\mathcal{M}} = \emptyset)$
$\mathbf{t}_{\mathsf{m}} \xleftarrow{\$} \mathbb{Z}_q^k, \quad \mathbf{u}_{\mathsf{m}} \xleftarrow{\$} \mathbb{Z}_q^{2k}$	
Return $([\mathbf{t}_{\mathsf{m}}]_2, [\mathbf{u}_{\mathsf{m}}]_2)$	

Figure 7. Description of $\mathcal{B}'(\mathcal{G}_1, ([\mathbf{D}]_1, [\mathbf{F}]_1)$ interpolating between $\mathsf{G}_2^{''}$ and $\mathsf{G}_2^{'}$.

If $r_c = 0$ then h_1 is distributed as in $\mathsf{G}_{1,L}$; if r_c is random then h_1 is distributed as in G_2'.

Next we bound the difference between G_2' and G_2'' by the Q_{c}-fold $\mathcal{U}_{3k,2k}$-MDDH assumption in $\mathbb{G}_1$, where G_2'' is the same as $\mathsf{G}_2^{'}$ except that when answering CHAL with $\mathsf{m}_1^* = 0$, one picks a random $\mathbf{h}_0 \xleftarrow{\$} \mathbb{Z}_q^k$ for each query. And the difference between G_2' and G_2'' can be bounded by the Q_{c}-fold $\mathcal{U}_{3k,2k}$-MDDH assumption in $\mathbb{G}_1$. Formally, on receiving a Q_{c}-fold $\mathcal{U}_{3k,2k}$-MDDH challenge $([\mathbf{D}]_1, [\mathbf{F}]_1 := ([\mathbf{f}_1, \cdots, \mathbf{f}_{Q_{\mathsf{c}}}]_1)) \in \mathbb{G}_1^{3k\times 2k} \times \mathbb{G}_1^{3k\times Q_{\mathsf{c}}}$, where Q_{c} denotes the number of challenge queries, we construct a reduction $\mathcal{B}_2$ as in Figure 7.

For EVAL(m) queries, since $\mathbf{u}_{\mathsf{m}}$ is information-theoretically hidden by $\mathsf{RF}(\mathsf{m})$, here we just pick $\mathbf{u}_{\mathsf{m}}$ uniformly random.

For CHAL(m^*) queries, if $\mathsf{m}_1^* = 1$, G_2'' and G_2' are the same, if $\mathsf{m}_1^* = 0$, we write $\mathbf{f}_c := \begin{pmatrix} \overline{\mathbf{D}}\mathbf{w}_c \\ \underline{\mathbf{D}}\mathbf{w}_c + \mathbf{r}_c \end{pmatrix}$ for some $\mathbf{w}_c \in \mathbb{Z}_q^{2k}$, where $\mathbf{r}_c \in \mathbb{Z}_q^k$ is $\mathbf{0}$ if $[\mathbf{F}]_2$ is from the real $\mathcal{U}_{3k,2k}$-MDDH distribution, and $\mathbf{r}_c$ is random otherwise. Then, we have

$$\begin{aligned}\mathbf{h}_0 &:= \mathbf{X}_{\mathsf{m}^*\backslash 1}^\top \mathbf{h} + \underline{\mathbf{f}_c} = \mathbf{X}_{\mathsf{m}^*\backslash 1}^\top \mathbf{h} + \underline{\mathbf{D}}\mathbf{w}_c + \mathbf{r}_c = \mathbf{X}_{\mathsf{m}^*\backslash 1}^\top \mathbf{h} + \underline{\mathbf{D}}\overline{\mathbf{D}}^{-1}\overline{\mathbf{f}_c} + \mathbf{r}_c \\ &= \underbrace{(\mathbf{X}_{\mathsf{m}^*\backslash 1}^\top + \underline{\mathbf{D}}\overline{\mathbf{D}}^{-1})}_{\mathbf{X}_{\mathsf{m}^*}^\top}\overline{\mathbf{f}_c} + \mathbf{r}_c.\end{aligned}$$

If $\mathbf{r}_c = \mathbf{0}$ then $\mathbf{h}_0$ is distributed as in G_2'; if $\mathbf{r}_c$ is random then $\mathbf{h}_0$ is distributed as in G_2''. The difference between G_2'' and G_2 can be bounded by the Q_{c}-fold $\mathcal{U}_{3k,2k}$-MDDH assumption in a similar way. □

□

We perform all the previous changes of Figure 2 in a reverse order without changing the simulation of CHAL. Then we have the following lemma.

Lemma 13 (G_2 to G_3). *If the $\mathcal{U}_{3k,k}$-MDDH problem is (t_2, ε_2)-hard in $\mathbb{G}_2$, then $|\Pr[\mathsf{G}_2^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathsf{mPR\text{-}CMA}_1^{\mathcal{A}} \Rightarrow 1]| \leq L\varepsilon_2 + 2^{-\Omega(\lambda)}$ and $t_1 \approx t_2 \approx t_{\mathcal{A}} + (Q_{\mathsf{e}} + Q_{\mathsf{c}})\mathsf{poly}(\lambda)$, where $\mathsf{poly}(\lambda)$ is independent of $t_{\mathcal{A}}$.*

By observing G_3 is the same as $\mathsf{mPR\text{-}CMA}_1$, we sum up Lemmata 4 to 13 and conclude Theorem 1. □

4 Quasi-adaptive Zero-knowledge Arguments for Linear Subspaces

4.1 Definition

The notion of quasi-adaptive non-interactive zero-knowledge arguments (QANIZK) is proposed by Jutla and Roy [33], where the common reference string CRS depends on the specific language for which proofs are generated. In the following we define a tag-based variant of QANIZK [34,17]. For simplicity, we only consider arguments for linear subspaces.

Let par be the public parameters for QANIZK and $\mathcal{D}_{\mathsf{par}}$ be a probability distribution over a collection of relations $R = \{R_{[\mathbf{M}]_1}\}$ parametrized by a matrix $[\mathbf{M}]_1 \in \mathbb{G}_1^{n\times t}$ $(n > t)$ with associated language $\mathcal{L}_{[\mathbf{M}]_1} = \{[\mathbf{c}_0]_1 : \exists \mathbf{r} \in \mathbb{Z}_q^t, \text{ s.t. } [\mathbf{c}_0]_1 = [\mathbf{M}\mathbf{r}]_1\}$. We consider witness sampleable distributions [33] where there is an efficiently sampleable distribution $\mathcal{D}'_{\mathsf{par}}$ outputs $\mathbf{M}' \in \mathbb{Z}_q^{n\times t}$ such that $[\mathbf{M}']_1$ distributes the same as $[\mathbf{M}]_1$. We note that the matrix distribution in Definition 2 is sampleable.

Definition 8 (Tag-based QANIZK). *A tag-based quasi-adaptive non-interactive zero-knowledge argument (QANIZK) for a language distribution $\mathcal{D}_{\mathsf{par}}$ consists of four PPT algorithms $\Pi = (\mathsf{Gen}_{\mathsf{NIZK}}, \mathsf{Prove}, \mathsf{Ver}_{\mathsf{NIZK}}, \mathsf{Sim})$.*

- *The key generation algorithm $\mathsf{Gen}_{\mathsf{NIZK}}(\mathsf{par}, [\mathbf{M}]_1)$ returns a common reference string crs and the trapdoor td, where crs defines a tag space $\mathcal{T}$.*
- *The proving algorithm $\mathsf{Prove}(\mathsf{crs}, \mathsf{tag}, [\mathbf{c}_0]_1, \mathbf{r})$ returns a proof π.*
- *The deterministic verification algorithm $\mathsf{Ver}_{\mathsf{NIZK}}(\mathsf{crs}, \mathsf{tag}, [\mathbf{c}_0]_1, \pi)$ returns 1 or 0, where 1 indicates that π is a valid proof for $[\mathbf{c}_0]_1 \in \mathcal{L}_{[\mathbf{M}]_1}$.*
- *The simulation algorithm $\mathsf{Sim}(\mathsf{crs}, \mathsf{td}, \mathsf{tag}, [\mathbf{c}_0]_1)$ returns a proof π for $[\mathbf{c}_0]_1 \in \mathcal{L}_{[\mathbf{M}]_1}$.*

(Perfect Completeness.) For all λ, all $[\mathbf{M}]_1$, all $([\mathbf{c}_0]_1, \mathbf{r})$ with $[\mathbf{c}_0]_1 = [\mathbf{M}\mathbf{r}]_1$, all $(\mathsf{crs}, \mathsf{td}) \in \mathsf{Gen}_{\mathsf{NIZK}}(\mathsf{par}, [\mathbf{M}]_1)$, and all $\pi \in \mathsf{Prove}(\mathsf{crs}, \mathsf{tag}, [\mathbf{c}_0]_1, \mathbf{r})$, we have $\mathsf{Ver}_{\mathsf{NIZK}}(\mathsf{crs}, \mathsf{tag}, [\mathbf{c}_0]_1, \pi) = 1$.

We require Π to have the following security. Here we require a stronger version of unbounded simulation soundness than the usual one in [34,17], where an adversary is allowed to submit a forgery with a reused tag.

Definition 9 (Perfect Zero-Knowledge). *A tag-based QANIZK Π is perfectly zero-knowledge if for all λ, all $[\mathbf{M}]_1$, all $([\mathbf{c}_0]_1, \mathbf{r})$ with $[\mathbf{c}_0]_1 = [\mathbf{M}\mathbf{r}]_1$, and all $(\mathsf{crs}, \mathsf{td}) \in \mathsf{Gen}_{\mathsf{NIZK}}(\mathsf{par}, [\mathbf{M}]_1)$, the following two distributions are identical:*

$$\mathsf{Prove}(\mathsf{crs}, \mathsf{tag}, [\mathbf{c}_0]_1, \mathbf{r}) \quad \textit{and} \quad \mathsf{Sim}(\mathsf{crs}, \mathsf{td}, \mathsf{tag}, [\mathbf{c}_0]_1).$$

Definition 10 (Unbounded Simulation Soundness.). *A tag-based QANIZK Π is $(Q_{\mathsf{s}}, t, \varepsilon)$-unbounded simulation sound (USS) if for any adversary $\mathcal{A}$ that runs in time t, it holds that $\Pr[\mathsf{USS}^{\mathcal{A}} \Rightarrow 1] \leq \varepsilon$, where Game USS is defined in Figure 8.*

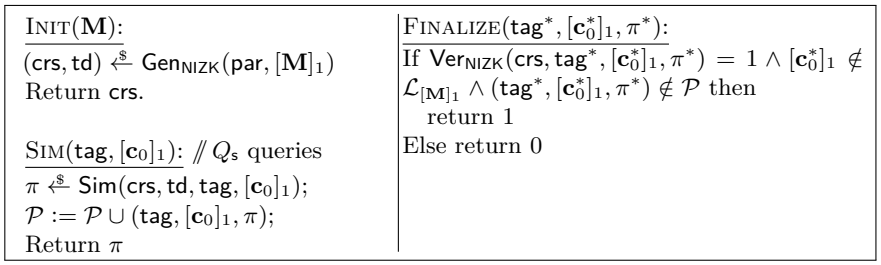

Figure 8. USS security game for QANIZK

4.2 Construction: QANIZK with unbounded simulation soundness

We (slightly) modify the QANIZK scheme in [17] to achieve our stronger unbounded simulation soundness (as in Definition 10). Let $\mathsf{par} := (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e, H)$ be the system parameter, where $H : \mathcal{T} \times \mathbb{G}_1^{n+k} \to \{0,1\}^\lambda$ is chosen uniformly from a collision-resistant hash function family $\mathcal{H}$. Our QANIZK scheme Π is defined as in Figure 9.

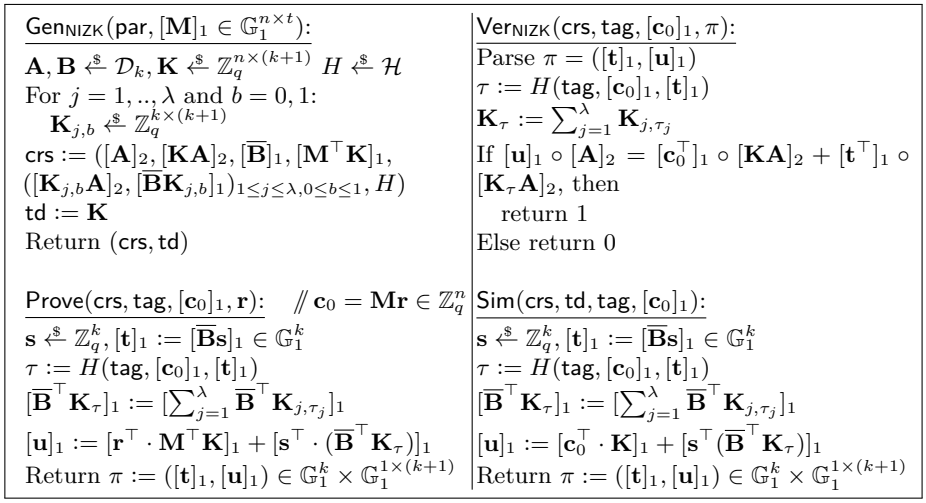

Figure 9. Construction of Π_{uss}.

Theorem 2. *The QANIZK system Π_{uss} defined in Figure 9 has perfect completeness and perfect zero-knowledge. Suppose in addition that the distribution of matrix $\mathbf{M}$ is witness sampleable, the $\mathcal{D}_k$-MDDH is (t_1, ε_1)-hard in $\mathbb{G}_1$, the $\mathcal{D}_k$-KerMDH is (t_2, ε_2)-hard in $\mathbb{G}_2$, $\mathcal{H}$ is a (t_3, ε_3)-collision resistant hash function family, then Π_{uss} is (t, ε)-USS, where $t_1 \approx t_2 \approx t_3 \approx t + Q_s\mathsf{poly}(\lambda)$, and $\varepsilon \leq \varepsilon_2 + 4\lambda\varepsilon_1 + \varepsilon_3 + 2^{-\Omega(\lambda)}$, $\mathsf{poly}(\lambda)$ is a polynomial independent of t.*

The proof is similar to that of [17] and we give the formal proof in the full version.

5 Identity-based Key Encapsulation Mechanism

We give our generic construction of an identity-based key encapsulation mechanism (IBKEM) from an affine MAC. Here we only focus on IBKEMs, since, even in the multi-instance, multi-challenge setting, a constrained CCA (resp. CPA) secure IBKEM can be transformed to a CCA (resp. CPA) secure identity-based encryption (IBE) in an efficient and tightly secure way by using an authenticated symmetric encryption scheme. One can prove this by adapting the known techniques from [30,20] in a straightforward way.

5.1 Definition

Let par be a set of system parameters.

Definition 11 (Identity-based key encapsulation mechanism). *An identity-based key encapsulation mechanism (IBKEM) has four algorithms* $\mathsf{IBKEM} := (\mathsf{Setup}, \mathsf{Ext}, \mathsf{Enc}, \mathsf{Dec})$ *with the following properties:*

- *The 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* $\mathcal{ID}$*, a symmetric key space* $\mathcal{K}$*, and a ciphertext space* $\mathcal{C}$*.*
- *The user secret-key generation algorithm* $\mathsf{Ext}(\mathsf{sk}, \mathsf{id})$ *returns a user secret key* $\mathsf{usk}[\mathsf{id}]$ *for an identity* $\mathsf{id} \in \mathcal{ID}$*.*
- *The encapsulation algorithm* $\mathsf{Enc}(\mathsf{pk}, \mathsf{id})$ *returns a 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 rejection symbol* $\perp$*.*

(Perfect correctness) *We require that for all pairs* $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\$} \mathsf{Setup}(\mathsf{par})$*, all identities* $\mathsf{id} \in \mathcal{ID}$*, all* $\mathsf{usk}[\mathsf{id}] \xleftarrow{\$} \mathsf{Ext}(\mathsf{sk}, \mathsf{id})$ *and all* $(\mathsf{K}, \mathsf{C}) \xleftarrow{\$} \mathsf{Enc}(\mathsf{pk}, \mathsf{id})$*,* $\Pr[\mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id}, \mathsf{C}) = \mathsf{K}] = 1$.

We define indistinguishability against constrained chosen-ciphertext and chosen-identity attacks for IBKEM in the multi-challenge setting.

Definition 12 ($\mathsf{mID\text{-}CCCA}$ security). *An identity-based key encapsulation scheme* IBKEM *is* $(Q_{\mathsf{ext}}, Q_{\mathsf{enc}}, Q_{\mathsf{dec}}, t, \varepsilon)$*-*$\mathsf{mID\text{-}CCCA}$*-secure if for all* $\mathcal{A}$ *with negligible* $\mathsf{uncert}(\mathcal{A})$ *that runs in time* t*, makes at most* Q_{ext} *user secret-key queries,* Q_{enc} *encryption queries and* Q_{dec} *decryption queries,*

$$|\Pr[\mathsf{mID\text{-}CCCA}_0^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathsf{mID\text{-}CCCA}_1^{\mathcal{A}} \Rightarrow 1]| \leq \varepsilon,$$

where the security game is defined as in Figure 10, here $\mathsf{pred}_i : \mathcal{K} \to \{0,1\}$ *denotes the predicate sent in the* i*th decryption query, the* uncertainty of knowledge about keys *corresponding to decryption queries is defined as*

$$\mathsf{uncert}(\mathcal{A}) := \frac{1}{Q_{\mathsf{dec}}} \sum_{i=1}^{Q_{\mathsf{dec}}} \Pr_{\mathsf{K} \xleftarrow{\$} \mathcal{K}}[\mathsf{pred}_i(\mathsf{K}) = 1].$$

INIT:	ENC(id^*): // at most Q_{enc} queries
$(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\$} \mathsf{Setup}(\mathsf{par})$	$\mathcal{Q}_{\mathsf{enc}} := \mathcal{Q}_{\mathsf{enc}} \cup \{\mathsf{id}^*\}$
Return pk	$(\mathsf{C}, \mathsf{K}) \xleftarrow{\$} \mathsf{Enc}(\mathsf{pk}, \mathsf{id}^*)$
	$\mathsf{K} \xleftarrow{\$} \mathcal{K}$
DEC($\mathsf{id}_i, \mathsf{C}_i, \mathsf{pred}_i$): // at most Q_{dec} queries	Return (C, K)
$\mathsf{usk}[\mathsf{id}_i] \xleftarrow{\$} \mathsf{Ext}(\mathsf{sk}, \mathsf{id}_i)$	
$\mathsf{K}_i \leftarrow \mathsf{Dec}(\mathsf{usk}[\mathsf{id}_i], \mathsf{id}_i, \mathsf{C}_i)$	EXT(id): // at most Q_{ext} queries
If $(\mathsf{id}_i, \mathsf{C}_i) \notin \mathcal{C}_{\mathsf{enc}}$ and $\mathsf{pred}_i(\mathsf{K}_i) = 1$ then	$\mathcal{Q}_{\mathsf{usk}} := \mathcal{Q}_{\mathsf{usk}} \cup \{\mathsf{id}\}$
return K_i	If $\mathsf{usk}[\mathsf{id}] = \bot$ then
Else return $\bot$	$\mathsf{usk}[\mathsf{id}] \xleftarrow{\$} \mathsf{Ext}(\mathsf{sk}, \mathsf{id})$
	Return $\mathsf{usk}[\mathsf{id}]$
FINALIZE(d):	
Return $d \wedge (\mathcal{Q}_{\mathsf{usk}} \cap \mathcal{Q}_{\mathsf{enc}} = \emptyset)$	

Figure 10. Games $\mathsf{mID\text{-}CCCA}_0$ and $\mathsf{mID\text{-}CCCA}_1$ for defining mID-CCCA-security.

If an adversary is not allowed to query DEC, then we get the security notion of indistinguishability against chosen-plaintext and chosen-identity attacks.

Definition 13 (mID-CPA security). *An identity-based key encapsulation scheme* IBKEM *is* $(Q_{\mathsf{ext}}, Q_{\mathsf{enc}}, t, \varepsilon)$-mID-CPA-*secure if* IBKEM *is* $(Q_{\mathsf{ext}}, Q_{\mathsf{enc}}, 0, t, \varepsilon)$-mID-CCCA-*secure.*

*Remark 1 (*EXT *queries with the same identity).* For simplicity, we assume that an adversary can query EXT with the same identity at most once. This is without loss of generality when assuming that the scheme is made deterministic, e.g., by generating the randomness in EXT with a (tightly secure) pseudorandom function such as the Naor-Reingold PRF [40]. Thus the anonymity we achieve here is usually called weak anonymity [22].

Remark 2 (On $\mathsf{uncert}(\mathcal{A})$*).* When we prove the IND-CCA security of the hybrid IBE scheme by combining an IND-CCCA secure ID-KEM together with an unconditionally one-time secure authenticated encryption scheme AE, the term $(Q_{\mathsf{dec}} + Q_{\mathsf{enc}})\mathsf{uncert}(\mathcal{A})$ is related to the one-time integrity of AE and can be made exponentially small (since it does not necessarily rely on any computational assumption). Hence, in line with previous works (e.g., [17]), we still call our reduction (almost) tight.

5.2 Two Transformations

We construct two generic transformations of IBKEM from affine MACs, IBKEM_1 and IBKEM_2. Let $\mathsf{par} := (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, P_1, P_2, e)$, $\mathsf{MAC} := (\mathsf{Gen}_{\mathsf{MAC}}, \mathsf{Tag}, \mathsf{Ver}_{\mathsf{MAC}})$ be an affine MAC and $\Pi := (\mathsf{Gen}_{\mathsf{NIZK}}, \mathsf{Prove}, \mathsf{Ver}_{\mathsf{NIZK}}, \mathsf{Sim})$ be a QANIZK system for linear language $\mathcal{L}_{[\mathbf{M}]_1} := \{[\mathbf{c}_0]_1 : \exists \mathbf{r} \in \mathbb{Z}_q^k \text{ s.t. } \mathbf{c}_0 = \mathbf{M}\mathbf{r}\}$, where $\mathbf{M} \in \mathcal{U}_{k+\eta,k}$. Our IBKEMs IBKEM_1 and IBKEM_2 are defined in Figure 11.

It is worth mentioning that if we instantiate our schemes with the SXDH assumption then we have: 4 elements in user secret keys, 4 elements in ciphertexts, and $(2\lambda + 4)$ elements in master public keys for IBKEM_1 (which is denoted by

$(|\mathsf{usk}|, |\mathsf{C}|, |\mathsf{pk}|) = (4, 4, 2\lambda + 4))$; and $(|\mathsf{usk}|, |\mathsf{C}|, |\mathsf{pk}|) = (4, 7, 8\lambda + 12)$ for IBKEM_2. We give concrete instantiations in the full version based on the MDDH and SXDH assumptions, respectively.

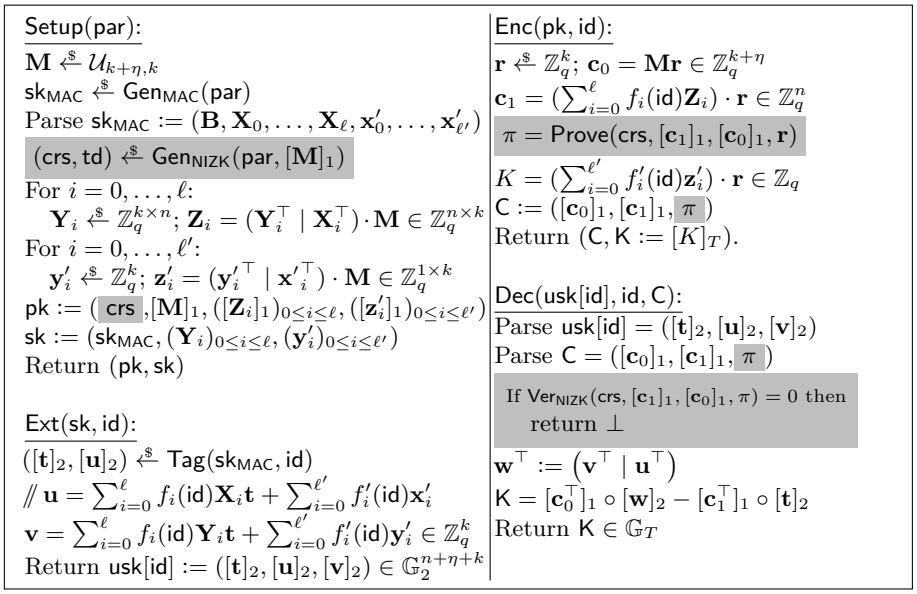

Figure 11. IBKEM_1 and IBKEM_2. Gray instructions are only executed in IBKEM_2.

IBKEM_1 is mID-CPA-secure and it follows the same idea as $\mathsf{IBE}[\mathsf{MAC}, \mathcal{D}_k]$ in [8]. Since our underlying MAC is secure in the multi-challenge setting, IBKEM_1 is ID-CPA-secure in the multi-challenge setting, and it can be also viewed as an alternative abstraction of [22] in the BKP framework.

The difficulty for IBKEM_1 to achieve mID-CCCA security is that decryption answers may leak information about $\mathsf{usk}[\mathsf{id}]$ for challenge id. We observe that if ciphertexts satisfy that $(\mathbf{c}_0 = \mathbf{M}\mathbf{r}) \wedge (\mathbf{c}_1 = (\sum_{i=0}^{\ell} f_i(\mathsf{id})\mathbf{Z}_i) \cdot \mathbf{r})$ for some $\mathbf{r}$ (we call such ciphertexts as "well-formed"), then the decrypted K reveals no more information about $\mathsf{usk}[\mathsf{id}]$ than pk. Since "$\mathbf{c}_0 \in \mathsf{Span}(\mathbf{M})$" is a linear statement, we can introduce the efficient unbounded simulation-sound QANIZK from Section 4 to reject DEC queries with $[\mathbf{c}_0]_1 \notin \mathsf{Span}([\mathbf{M}]_1)$. Furthermore, due to the randomness contained in $\mathsf{usk}[\mathsf{id}]$, if $\mathbf{c}_0 \in \mathsf{Span}(\mathbf{M})$ but $\mathbf{c}_1$ is not "well-formed", the decrypted K will be randomly distributed and thus it will be rejected by the decryption oracle. Note that $[\mathbf{c}_1]_1$ works as the tag for QANIZK argument. We refer the proof of Theorem 4 for technical details.

Theorem 3 (mID-CPA **Security of** IBKEM_1)**.** *If the* $\mathcal{U}_k$-MDDH *is* (t_1, ε_1)*-hard in* $\mathbb{G}_1$*, and* MAC *is a* $(Q_{\mathsf{e}}, Q_{\mathsf{c}}, t_2, \varepsilon_2)$-mPR-CMA*-secure affine MAC, then* IBKEM_1 *is* $(Q_{\mathsf{ext}}, Q_{\mathsf{enc}}, t, \varepsilon)$-mID-CPA*-secure, where* $Q_{\mathsf{ext}} \le Q_{\mathsf{e}}, Q_{\mathsf{enc}} \le Q_{\mathsf{c}}$*,* $t_1 \approx t_2 \approx t + (Q_{\mathsf{ext}} + Q_{\mathsf{enc}})\mathsf{poly}(\lambda)$ *and* $\varepsilon \le 2(\varepsilon_1 + \varepsilon_2 + 2^{-\Omega(\lambda)})$.

The proof of Theorem 3 is an extension of Theorem 4.3 in [8] in the multi-challenge setting. We leave the proof in the full version.

Theorem 4 (mID-CCCA Security of IBKEM_2). *If the $\mathcal{U}_k$-MDDH is (t_1, ε_1)-hard in $\mathbb{G}_1$, MAC is a $(Q_\mathsf{e}, Q_\mathsf{c}, t_2, \varepsilon_2)$-mPR-CMA-secure affine MAC, Π is a $(Q_\mathsf{s}, t_3, \varepsilon_3)$-USS QANIZK, then IBKEM_2 is $(Q_\mathsf{ext}, Q_\mathsf{enc}, Q_\mathsf{dec}, t, \varepsilon)$-mID-CCCA-secure, where $Q_\mathsf{ext} \leq Q_\mathsf{e}$, $Q_\mathsf{enc} \leq Q_\mathsf{c} \approx Q_\mathsf{s}$, $t_3 \approx t_1 \approx t_2 \approx t + (Q_\mathsf{dec} + Q_\mathsf{enc} + Q_\mathsf{ext})\mathsf{poly}(\lambda)$ and $\varepsilon \leq 2(\varepsilon_1 + \varepsilon_2 + \varepsilon_3 + 2Q_\mathsf{dec} \cdot \mathsf{uncert}(\mathcal{A}) + 2^{-\Omega(\lambda)})$.*

It is easy to verify the correctness of IBKEM_1 and IBKEM_2.

Proof (of Theorem 4). We define a series of games in Figure 12 to prove the mID-CCCA security of IBKEM_2. A brief overview of game changes is described as in Figure 13. For a simple presentation of Figure 12, we define $\mathbf{X}_\mathsf{id} := \sum_{i=0}^{\ell} f_i(\mathsf{id})\mathbf{X}_i$, $\mathbf{Y}_\mathsf{id} := \sum_{i=0}^{\ell} f_i(\mathsf{id})\mathbf{Y}_i$, $\mathbf{Z}_\mathsf{id} := \sum_{i=0}^{\ell} f_i(\mathsf{id})\mathbf{Z}_i$, $\mathbf{x}'_\mathsf{id} := \sum_{i=0}^{\ell'} f'_i(\mathsf{id})\mathbf{x}'_i$, $\mathbf{y}'_\mathsf{id} := \sum_{i=0}^{\ell'} f'_i(\mathsf{id})\mathbf{y}'_i$, $\mathbf{z}'_\mathsf{id} := \sum_{i=0}^{\ell'} f'_i(\mathsf{id})\mathbf{z}'_i$ for an $\mathsf{id} \in \{0,1\}^L$.

Lemma 14 (G_0 to G_1). $\Pr[\mathsf{mID\text{-}CCCA}_0^\mathcal{A} \Rightarrow 1] = \Pr[\mathsf{G}_0^\mathcal{A} \Rightarrow 1] = \Pr[\mathsf{G}_1^\mathcal{A} \Rightarrow 1]$

Proof. G_0 is the real attack game. In 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:

$$\mathbf{c}_1 = \mathbf{Z}_{\mathsf{id}^*}\mathbf{r} = (\mathbf{Y}_{\mathsf{id}^*}^\top \mid \mathbf{X}_{\mathsf{id}^*}^\top)\mathbf{M}\mathbf{r} = (\mathbf{Y}_{\mathsf{id}^*}^\top \mid \mathbf{X}_{\mathsf{id}^*}^\top)\mathbf{c}_0$$

and $K = (\mathbf{y}'^\top_{\mathsf{id}^*} \mid \mathbf{x}'^\top_{\mathsf{id}^*})\mathbf{M}\mathbf{r} = (\mathbf{y}'_{\mathsf{id}^*}{}^\top \mid \mathbf{x}'_{\mathsf{id}^*}{}^\top)\mathbf{c}_0$. This change is only conceptual. Moreover, we simulate the QANIZK proof π in $\textsc{Enc}(\mathsf{id}^*)$ by using Π's zero-knowledge simulator. By the perfect zero-knowledge property of Π, G_1 is identical to G_0. □

Lemma 15 (G_1 to G_2). *If the $\mathcal{U}_{k+\eta,k}$-MDDH problem is (t_1, ε_1)-hard in $\mathbb{G}_1$, then $|\Pr[\mathsf{G}_1^\mathcal{A} \Rightarrow 1] - \Pr[\mathsf{G}_2^\mathcal{A} \Rightarrow 1]| \leq \varepsilon_1 + 2^{-\Omega(\lambda)}$ and $t_1 \approx t_\mathcal{A} + (Q_\mathsf{dec} + Q_\mathsf{enc} + Q_\mathsf{ext})\mathsf{poly}(\lambda)$, where poly is a polynomial independent of $t_\mathcal{A}$.*

Lemma 15 can be proved by a straightforward reduction to the Q_enc-fold $\mathcal{U}_{k+\eta,k}$-MDDH problem in $\mathbb{G}_1$ and we omit it here.

Lemma 16 (G_2 to G_3). *If the tag-based QANIZK Π is $(Q_\mathsf{s}, t_3, \varepsilon_3)$-USS, then $|\Pr[\mathsf{G}_2^\mathcal{A} \Rightarrow 1] - \Pr[\mathsf{G}_3^\mathcal{A} \Rightarrow 1]| \leq \varepsilon_3 + Q_\mathsf{dec}\mathsf{uncert}(\mathcal{A})$ and $Q_\mathsf{s} \geq Q_\mathsf{enc}$, $t_3 \approx t_\mathcal{A} + (Q_\mathsf{dec} + Q_\mathsf{ext} + Q_\mathsf{enc})\mathsf{poly}(\lambda)$, where poly is a polynomial independent of $t_\mathcal{A}$.*

Proof. The difference between G_2 and G_3 happens when an adversary queries the decryption oracle $\textsc{Dec}$ with $(\mathsf{id}, \mathsf{C} = ([\mathbf{c}_0]_1, [\mathbf{c}_1]_1, \pi), \mathsf{pred})$ where $\mathsf{id} \notin \mathcal{Q}_\mathsf{usk} \wedge \mathsf{pred}(\mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id}, \mathsf{C})) = 1 \wedge \mathbf{c}_0 \notin \mathsf{Span}(\mathbf{M}) \wedge \mathsf{Ver}_\mathsf{NIZK}(\mathsf{crs}, [\mathbf{c}_1]_1, [\mathbf{c}_0]_1, \pi) = 1$. That is bounded by the unbounded simulation soundness (USS) of Π. Formally, we construct an algorithm $\mathcal{B}$ in Figure 14 to break the USS of Π and we highlight the important steps with gray.

We analyze the success probability of $\mathcal{B}$. For a $\textsc{Dec}(\mathsf{id}, \mathsf{C}, \mathsf{pred}_i)$ query, we have the following two cases:

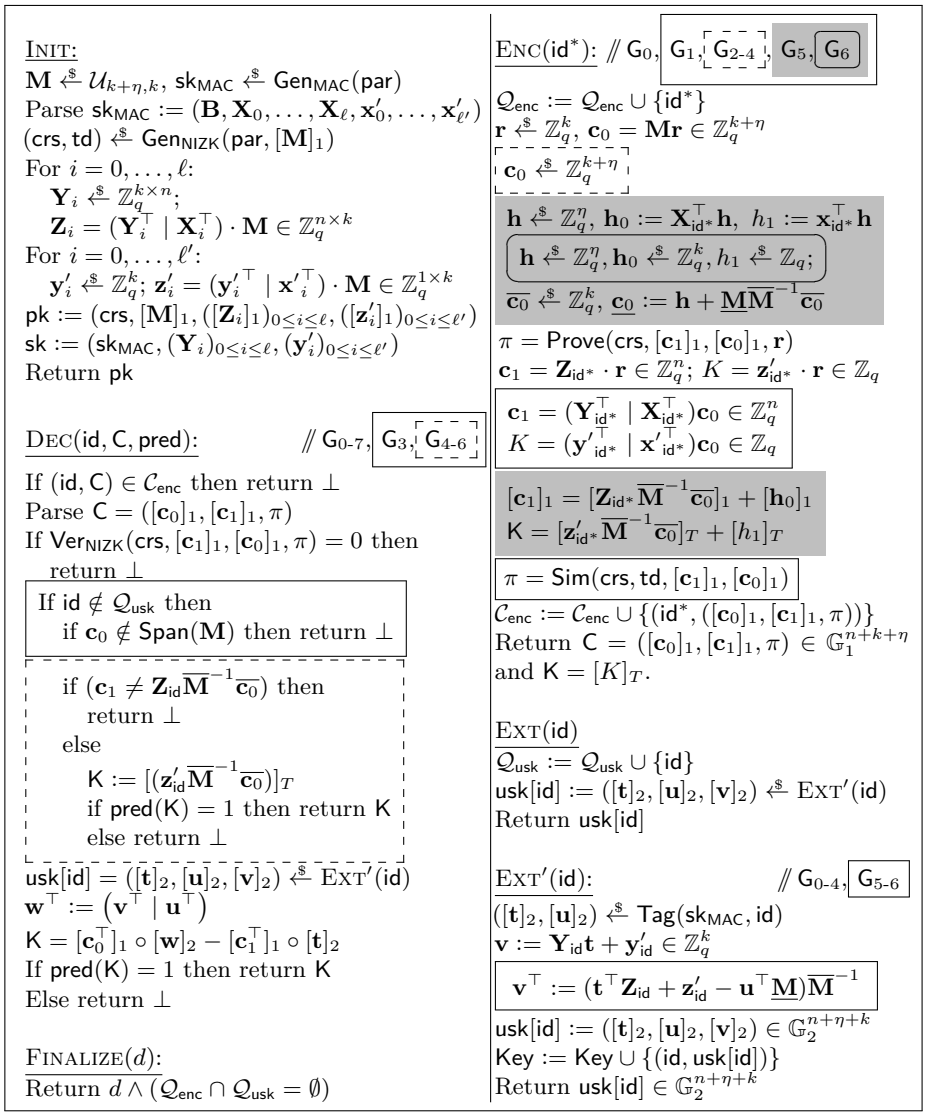

Figure 12. Games G_0-G_6 for the proof of Theorem 4.

– $([\mathbf{c}_1]_1, [\mathbf{c}_0]_1, \pi) = ([\mathbf{c}_1^*]_1, [\mathbf{c}_0^*]_1, \pi^*)$ for some $(\mathsf{id}^*, \mathsf{C}^*) \in \mathcal{C}_{\mathsf{enc}}$ with $\mathsf{id} \neq \mathsf{id}^*$. In this case, $\mathcal{B}$ cannot break the USS property, but the adversary $\mathcal{A}$ can ask such a query with $\mathsf{pred}_i(\mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id}, \mathsf{C})) = 1$ with probability $\mathsf{uncert}(\mathcal{A})$.

#	modification	remarks
G_0	the same as $\mathsf{mID\text{-}CCCA}_0$	-
G_1	ENC : compute $\mathbf{c}_1, \mathsf{K}$ with sk,π with td	ZK of Π
G_2	ENC : $\mathbf{c}_0 \xleftarrow{\$} \mathbb{Z}_q^{k+\eta}$	$\mathcal{U}_{k+\eta,k}$-MDDH in $\mathbb{G}_1$
G_3	DEC: for $\mathsf{id} \notin \mathcal{Q}_{\mathsf{usk}}$, reject C with $\mathbf{c}_0 \notin \mathsf{Span}(\mathbf{M})$	USS of Π
G_4	DEC: for $\mathsf{id} \notin \mathcal{Q}_{\mathsf{usk}}$, reject C with $\mathbf{c}_1 \neq \mathbf{Z}_{\mathsf{id}}\overline{\mathbf{M}}^{-1}\overline{\mathbf{c}_0}$	entropy of $\mathbf{t}$
G_5	EXT, ENC : compute $\mathbf{c}_1, K$ and $\mathbf{v}$ with pk and $\mathsf{sk}_{\mathsf{MAC}}$	-
G_6	ENC: $\mathbf{c}_1 \xleftarrow{\$} \mathbb{Z}_q^k, K \xleftarrow{\$} \mathbb{Z}_q$	mPR-CMA of MAC

Figure 13. Overview of game changes for proof of Theorem 4

More precisely, we have

$$\begin{aligned}\mathsf{K} &= [\mathbf{c}_0^\top]_1 \circ [\mathbf{w}]_2 - [\mathbf{c}_1^\top]_1 \circ [\mathbf{t}]_2 \\ &= [\mathbf{c}_0^\top]_1 \circ [\mathbf{w}]_2 - [\mathbf{c}_0^\top(\mathbf{Y}_{\mathsf{id}^*} \mid \mathbf{X}_{\mathsf{id}^*})]_1 \circ [\mathbf{t}]_2 \\ &= [\mathbf{c}_0^\top]_1 \circ [(\mathbf{Y}_{\mathsf{id}} \mid \mathbf{X}_{\mathsf{id}})\mathbf{t}]_2 - [\mathbf{c}_0^\top(\mathbf{Y}_{\mathsf{id}^*} \mid \mathbf{X}_{\mathsf{id}^*})]_1 \circ [\mathbf{t}]_2 \\ &= [\mathbf{c}_0^\top]_1 \circ [(\mathbf{Y}_\Delta \mid \mathbf{X}_\Delta)\mathbf{t}]_2,\end{aligned}$$

where $\mathbf{Y}_\Delta := \mathbf{Y}_{\mathsf{id}} - \mathbf{Y}_{\mathsf{id}^*}$ and $\mathbf{X}_\Delta := \mathbf{X}_{\mathsf{id}} - \mathbf{X}_{\mathsf{id}^*}$. By $\mathsf{id} \notin \mathcal{Q}_{\mathsf{usk}}$, the corresponding $\mathbf{t}$ is randomly distributed in the adversary's view. Clearly, $(\mathbf{Y}_\Delta \mid \mathbf{X}_\Delta) \neq \mathbf{0}$, since $\mathsf{id} \neq \mathsf{id}^*$. Thus, K is randomly distributed and $\mathcal{A}$ can output a pred_i such that $\mathsf{pred}_i(\mathsf{K}) = 1$ with probability $\mathsf{uncert}(\mathcal{A})$.

– $([\mathbf{c}_1]_1, [\mathbf{c}_0]_1, \pi) \neq ([\mathbf{c}_1^*]_1, [\mathbf{c}_0^*]_1, \pi^*)$ for all $(\mathsf{id}^*, \mathsf{C}^*) \in \mathcal{C}_{\mathsf{enc}}$. In this case, $([\mathbf{c}_1]_1, [\mathbf{c}_0]_1, \pi)$ is a valid proof to break the USS of Π.

To sum up, the success probability of $\mathcal{B}$ is at least $|\Pr[\mathsf{G}_2^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathsf{G}_3^{\mathcal{A}} \Rightarrow 1]| - Q_{\mathsf{dec}} \cdot \mathsf{uncert}(\mathcal{A})$. □

Lemma 17 (G_3 to G_4). $|\Pr[\mathsf{G}_3^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathsf{G}_4^{\mathcal{A}} \Rightarrow 1]| \leq Q_{\mathsf{dec}} \cdot \mathsf{uncert}(\mathcal{A})$.

Proof. An adversary $\mathcal{A}$ can distinguish G_4 from G_3 if $\mathcal{A}$ asks the decryption oracle DEC with $(\mathsf{id}, \mathsf{C} = ([\mathbf{c}_0]_1, [\mathbf{c}_1]_1, \pi), \mathsf{pred})$ where $\mathbf{c}_1 \neq \mathbf{Z}_{\mathsf{id}}\overline{\mathbf{M}}^{-1} \cdot \overline{\mathbf{c}_0}$ but $\mathsf{pred}(\mathsf{Dec}(\mathsf{usk}[\mathsf{id}], \mathsf{id}, \mathsf{C})) = 1$.

We show that, before an identity id is queried to EXT, for any $(\mathbf{c}_0, \mathbf{c}_1)$, the value $K = \mathbf{c}_0^\top \begin{pmatrix}\mathbf{v}_{\mathsf{id}} \\ \mathbf{u}_{\mathsf{id}}\end{pmatrix} - \mathbf{c}_1^\top \mathbf{t}_{\mathsf{id}}$ is uniformly random from the adversary's view, where $([\mathbf{t}_{\mathsf{id}}]_2, [\mathbf{u}_{\mathsf{id}}]_2, [\mathbf{v}_{\mathsf{id}}]_2) \in \mathrm{EXT}(\mathsf{id})$:

$$\begin{aligned}K = \mathbf{c}_0^\top \begin{pmatrix}\mathbf{v}_{\mathsf{id}} \\ \mathbf{u}_{\mathsf{id}}\end{pmatrix} - \mathbf{c}_1^\top \mathbf{t}_{\mathsf{id}} &= \mathbf{c}_0^\top \begin{pmatrix}((\mathbf{t}_{\mathsf{id}}^\top \mathbf{Z}_{\mathsf{id}} + \mathbf{z}'_{\mathsf{id}} - \mathbf{u}_{\mathsf{id}}^\top \cdot \underline{\mathbf{M}}) \cdot \overline{\mathbf{M}}^{-1})^\top \\ \mathbf{u}_{\mathsf{id}}\end{pmatrix} - \mathbf{c}_1^\top \mathbf{t}_{\mathsf{id}} \\ &= \overline{\mathbf{c}}_0^\top (\overline{\mathbf{M}}^{-1})^\top \mathbf{z}'^\top_{\mathsf{id}} + \underbrace{(\underline{\mathbf{c}_0^\top} - (\underline{\mathbf{M}}\overline{\mathbf{M}}^{-1}\overline{\mathbf{c}_0})^\top)}_{\Delta_1} \mathbf{u}_{\mathsf{id}} + \underbrace{((\mathbf{Z}_{\mathsf{id}} \cdot \overline{\mathbf{M}}^{-1} \cdot \overline{\mathbf{c}}_0)^\top - \mathbf{c}_1^\top)}_{\Delta_2} \mathbf{t}_{\mathsf{id}}\end{aligned}$$

In G_3 and G_4, a DEC query with $\mathbf{c}_0 \notin \mathsf{Span}(\mathbf{M})$ and $\mathsf{id} \notin \mathcal{Q}_{\mathsf{usk}}$ will be rejected, and thus we have $\Delta_1 = \mathbf{0}$. As id has never been queried to EXT, $\mathbf{t}_{\mathsf{id}}$ is uniformly

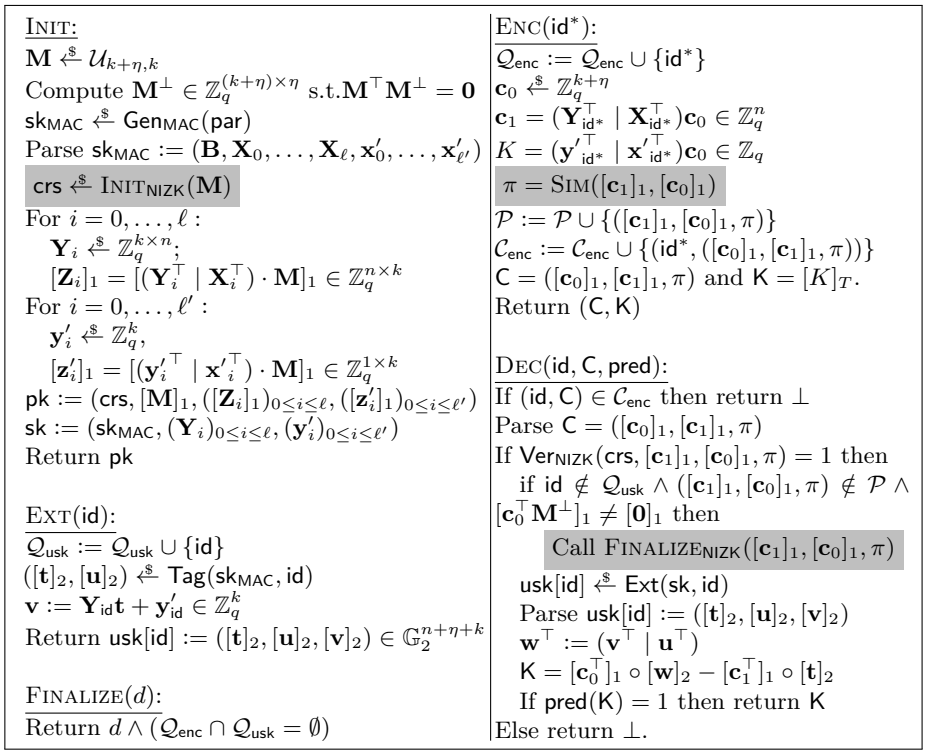

Figure 14. Description of $\mathcal{B}$ with oracle access to $\text{INIT}_{\mathsf{NIZK}}, \text{SIM}, \text{FINALIZE}_{\mathsf{NIZK}}$ of the USS games of Figure 8 for the proof of Lemma 16.

random to the adversary. Thus, if $\mathbf{c}_1 \neq \mathbf{Z}_{\mathsf{id}}\overline{\mathbf{M}}^{-1}\overline{\mathbf{c}_0}$ (namely, $\Delta_2 \neq \mathbf{0}$) then K is random and a query of this form will be rejected except with probability $\mathsf{uncert}(\mathcal{A})$. By the union bound, the difference between G_3 and G_4 is bounded by $Q_{\mathsf{dec}} \cdot \mathsf{uncert}(\mathcal{A})$. □

Lemma 18 (G_4 to G_5). $\Pr[\mathsf{G}_4^{\mathcal{A}} \Rightarrow 1] = \Pr[\mathsf{G}_5^{\mathcal{A}} \Rightarrow 1]$.

Proof. The change from G_4 to G_5 is only conceptual. By $\mathbf{Z}_i = (\mathbf{Y}_i^\top \mid \mathbf{X}_i^\top)\mathbf{M}$, we have $\mathbf{Y}_i^\top = (\mathbf{Z}_i - \mathbf{X}_i^\top \cdot \underline{\mathbf{M}}) \cdot (\overline{\mathbf{M}})^{-1}$, and similarly we have $\mathbf{y}'^\top_i = (\mathbf{z}'_i - \mathbf{x}'^\top_i \cdot \underline{\mathbf{M}}) \cdot \overline{\mathbf{M}}^{-1}$. For EXT(id), by substituting $\mathbf{Y}_i^\top$ and $\mathbf{y}'^\top_i$, we obtain

$$\begin{aligned}\mathbf{v}^\top &= \left(\mathbf{t}^\top(\mathbf{Z}_{\mathsf{id}} - \mathbf{X}_{\mathsf{id}}^\top \cdot \underline{\mathbf{M}}) + (\mathbf{z}'_{\mathsf{id}} - \mathbf{x}'^\top_{\mathsf{id}} \cdot \underline{\mathbf{M}})\right)\overline{\mathbf{M}}^{-1} \\ &= \left(\mathbf{t}^\top\mathbf{Z}_{\mathsf{id}} + \mathbf{z}'_{\mathsf{id}} - \underbrace{(\mathbf{t}^\top\mathbf{X}_{\mathsf{id}}^\top + \mathbf{x}'^\top_{\mathsf{id}})}_{\mathbf{u}^\top} \cdot \underline{\mathbf{M}}\right) \cdot \overline{\mathbf{M}}^{-1}\end{aligned}$$

Note that we can compute $[\mathbf{v}]_2$ in G_5, since $\mathbf{A}$, $\mathbf{z}'_i$ and $\mathbf{Z}_i$ are known explicitly over $\mathbb{Z}_q$ and $[\mathbf{t}]_2$ and $[\mathbf{u}]_2$ are known.

$\mathbf{c}_0$ from $\textsc{Enc}(\mathsf{id}^*)$ is uniformly random in G_4 and G_5. By $\mathbf{h} = \underline{\mathbf{c}_0} - \underline{\mathbf{M}} \cdot \overline{\mathbf{M}}^{-1}\overline{\mathbf{c}_0}$, we have

$$\begin{aligned}\mathbf{c}_1 &= \mathbf{Z}_{\mathsf{id}^*} \cdot \overline{\mathbf{M}}^{-1}\overline{\mathbf{c}_0} + \mathbf{X}_{\mathsf{id}^*}^\top \cdot (\underline{\mathbf{c}_0} - \underline{\mathbf{M}} \cdot \overline{\mathbf{M}}^{-1}\overline{\mathbf{c}_0}) \\ &= (\mathbf{Y}_{\mathsf{id}^*}^\top \overline{\mathbf{M}} + \mathbf{X}_{\mathsf{id}^*}^\top \underline{\mathbf{M}}) \cdot \overline{\mathbf{M}}^{-1}\overline{\mathbf{c}_0} + \mathbf{X}_{\mathsf{id}^*}^\top \cdot (\underline{\mathbf{c}_0} - \underline{\mathbf{M}} \cdot \overline{\mathbf{M}}^{-1}\overline{\mathbf{c}_0}) \\ &= (\mathbf{Y}_{\mathsf{id}^*}^\top \mid \mathbf{X}_{\mathsf{id}^*}^\top)\mathbf{c}_0\end{aligned}$$

and $\mathbf{c}_1$ is distributed as in G_4. The distribution of K can be proved by a similar argument. □

Lemma 19 (G_5 to G_6). *If* MAC *is* $(Q_\mathsf{e}, Q_\mathsf{c}, t_2, \varepsilon_2)$-mPR-CMA*-secure, then* $|\Pr[\mathsf{G}_5^{\mathcal{A}} \Rightarrow 1] - \Pr[\mathsf{G}_6^{\mathcal{A}} \Rightarrow 1]| \leq \varepsilon_2$ *with* $Q_{\mathsf{ext}} \leq Q_\mathsf{e}$, $Q_{\mathsf{enc}} \leq Q_\mathsf{c}$, $t_2 \approx t_{\mathcal{A}} + (Q_{\mathsf{dec}} + Q_{\mathsf{ext}} + Q_{\mathsf{enc}})\mathsf{poly}(\lambda)$*, where* poly *is a polynomial independent of* $t_{\mathcal{A}}$*.*

Proof. In G_6, we answer the $\textsc{Enc}(\mathsf{id})$ query by choosing random K and $([\mathbf{c}_0]_1, [\mathbf{c}_1]_1)$. We construct an adversary $\mathcal{D}$ in Figure 15 to bound the differences between G_5 and G_6 with the mPR-CMA security of MAC. The decryption oracle $\textsc{Dec}$ is simulated as in G_5 and G_6. Now if $\mathcal{D}$ is in $\mathsf{mPR\text{-}CMA}_1$ then the simulated distribution is identical to G_6; otherwise, it is identical to G_5. □

$\underline{\textsc{Init}:}$ $\mathbf{M} \xleftarrow{\$} \mathcal{U}_{k+\eta,k}$ Compute $\mathbf{M}^\perp \in \mathbb{Z}_q^{(k+\eta)\times\eta}$ s.t.$\mathbf{M}^\top\mathbf{M}^\perp = \mathbf{0}$ $\epsilon \xleftarrow{\$} \textsc{Init}_{\mathsf{MAC}}$ $(\mathsf{crs}, \mathsf{td}) \xleftarrow{\$} \mathsf{Gen}_{\mathsf{NIZK}}(\mathsf{par}, [\mathbf{M}]_1)$ For $i = 0, \ldots, \ell$: $\mathbf{Z}_i \xleftarrow{\$} \mathbb{Z}_q^{n\times k}$ For $i = 0, \ldots, \ell'$: $\mathbf{z}'_i \xleftarrow{\$} \mathbb{Z}_q^{1\times k}$ $\mathsf{pk} := (\mathsf{crs}, [\mathbf{M}]_1, ([\mathbf{Z}_i]_1)_{0\leq i\leq\ell}, ([\mathbf{z}'_i]_1)_{0\leq i\leq\ell'})$ Return pk $\underline{\textsc{Ext}(\mathsf{id}):}$ $\mathcal{Q}_{\mathsf{usk}} := \mathcal{Q}_{\mathsf{usk}} \cup \{\mathsf{id}\}$ $([\mathbf{t}]_2, [u]_2) \xleftarrow{\$} \textsc{Eval}(\mathsf{id})$ $\mathbf{v}^\top := (\mathbf{t}^\top\mathbf{Z}_{\mathsf{id}} + \mathbf{z}'_{\mathsf{id}} - \mathbf{u}^\top \cdot \underline{\mathbf{M}}) \cdot (\overline{\mathbf{M}})^{-1}$ Return $\mathsf{usk}[\mathsf{id}] := ([\mathbf{t}]_2, [\mathbf{u}]_2, [\mathbf{v}]_2) \in \mathbb{G}_2^{n+\eta+k}$	$\underline{\textsc{Enc}(\mathsf{id}^*):}$ $\mathcal{Q}_{\mathsf{enc}} := \mathcal{Q}_{\mathsf{enc}} \cup \{\mathsf{id}^*\}$ $([\mathbf{h}]_1, [\mathbf{h}_0]_1, [h_1]_T) \xleftarrow{\$} \textsc{Chal}(\mathsf{id}^*)$ $\overline{\mathbf{c}_0} \xleftarrow{\$} \mathbb{Z}_q^k$ $\underline{\mathbf{c}_0} := \mathbf{h} + \underline{\mathbf{M}} \cdot \overline{\mathbf{M}}^{-1}\overline{\mathbf{c}_0} \in \mathbb{Z}_q^\eta$ $\mathbf{c}_1 := \mathbf{Z}_{\mathsf{id}^*} \cdot \overline{\mathbf{M}}^{-1}\overline{\mathbf{c}_0} + \mathbf{h}_0$ $K := \mathbf{z}'_{\mathsf{id}^*} \cdot \overline{\mathbf{M}}^{-1}\overline{\mathbf{c}_0} + h_1$ $\pi := \mathsf{Sim}(\mathsf{crs}, \mathsf{td}, [\mathbf{c}_1]_1, [\mathbf{c}_0]_1)$ $\mathcal{C}_{\mathsf{enc}} := \mathcal{C}_{\mathsf{enc}} \cup \{(\mathsf{id}, ([\mathbf{c}_0]_1, [\mathbf{c}_1]_1, \pi))\}$ $\mathsf{C} := ([\mathbf{c}_0]_1, [\mathbf{c}_1]_1, \pi)$ and $\mathsf{K} := [K]_T$. Return (C, K) $\underline{\textsc{Finalize}(d):}$ Return $\textsc{Finalize}_{\mathsf{MAC}}(d) \wedge (\mathcal{Q}_{\mathsf{enc}} \cap \mathcal{Q}_{\mathsf{usk}} = \emptyset)$

Figure 15. Description of $\mathcal{D}$ (with access to oracles $\textsc{Init}_{\mathsf{MAC}}, \textsc{Eval}, \textsc{Chal}, \textsc{Finalize}_{\mathsf{MAC}}$ of the $\mathsf{mPR\text{-}CMA}_0/\mathsf{mPR\text{-}CMA}_1$ games of Figure 1) for the proof of Lemma 19.

We observe that G_6 is computationally indistinguishable from $\mathsf{mID\text{-}CCCA}_{\mathsf{rand}}$ by a reverse arguments of Lemmata 14 to 19 without changing the distribution of K in $\textsc{Enc}$. More precisely, we can argue this by switching the ciphertexts from random to real and removing all the additional rejection rules in $\textsc{Dec}$. Thus, we conclude Theorem 4. □

Remark 3 (Anonymity). In G_6 all the challenge ciphertexts are independent of the challenge identity id^*: $[\mathbf{c}_1]_1$ is uniform and $[\mathbf{c}_0]_1$ and π are independent of id^*. Thus, our scheme is trivially anonymous.

Acknowledgments. We thank the anonymous reviewers for their comments and, in particular, for pointing a problem in our definition of unbounded simulation soundness, and one in the proof of Theorem 4 in a previous version of this paper. The first author was supported by ERC Project PREP-CRYPTO (724307) and DFG grants (HO 4534/4-1, HO 4534/2-2), the second author was supported by the National Nature Science Foundation of China (Nos. 61502484, 61572495, 61772515) and the National Cryptography Development Fund (No. MMJJ20170116), and the third author was supported by the DFG grant (HO 4534/4-1). This work was done while the second author was visiting KIT. The visit was supported by China Scholarship Council.

References

1. Abe, M., David, B., Kohlweiss, M., Nishimaki, R., Ohkubo, M.: Tagged one-time signatures: Tight security and optimal tag size. In: Kurosawa, K., Hanaoka, G. (eds.) PKC 2013. LNCS, vol. 7778, pp. 312–331. Springer, Heidelberg (Feb / Mar 2013) 2
2. Abe, M., Hofheinz, D., Nishimaki, R., Ohkubo, M., Pan, J.: Compact structure-preserving signatures with almost tight security. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017, Part II. LNCS, vol. 10402, pp. 548–580. Springer, Heidelberg (Aug 2017) 2
3. Attrapadung, N., Hanaoka, G., Yamada, S.: A framework for identity-based encryption with almost tight security. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015, Part I. LNCS, vol. 9452, pp. 521–549. Springer, Heidelberg (Nov / Dec 2015) 2, 3
4. Auerbach, B., Cash, D., Fersch, M., Kiltz, E.: Memory-tight reductions. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017, Part I. LNCS, vol. 10401, pp. 101–132. Springer, Heidelberg (Aug 2017) 2
5. Bader, C., Hofheinz, D., Jager, T., Kiltz, E., Li, Y.: Tightly-secure authenticated key exchange. In: Dodis, Y., Nielsen, J.B. (eds.) TCC 2015, Part I. LNCS, vol. 9014, pp. 629–658. Springer, Heidelberg (Mar 2015) 2
6. Bellare, M., Boldyreva, A., Micali, S.: Public-key encryption in a multi-user setting: Security proofs and improvements. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 259–274. Springer, Heidelberg (May 2000) 1
7. Bellare, M., Goldwasser, S.: New paradigms for digital signatures and message authentication based on non-interative zero knowledge proofs. In: Brassard, G. (ed.) CRYPTO'89. LNCS, vol. 435, pp. 194–211. Springer, Heidelberg (Aug 1990) 3
8. Blazy, O., Kiltz, E., Pan, J.: (Hierarchical) identity-based encryption from affine message authentication. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014, Part I. LNCS, vol. 8616, pp. 408–425. Springer, Heidelberg (Aug 2014) 2, 3, 7, 9, 10, 13, 22, 23
9. Boneh, D., Canetti, R., Halevi, S., Katz, J.: Chosen-ciphertext security from identity-based encryption. SIAM J. Comput. 36(5), 1301–1328 (2007) 2
10. Boneh, D., Mironov, I., Shoup, V.: A secure signature scheme from bilinear maps. In: Joye, M. (ed.) CT-RSA 2003. LNCS, vol. 2612, pp. 98–110. Springer, Heidelberg (Apr 2003) 2
11. Chen, J., Gong, J., Weng, J.: Tightly secure IBE under constant-size master public key. In: Fehr, S. (ed.) PKC 2017, Part I. LNCS, vol. 10174, pp. 207–231. Springer, Heidelberg (Mar 2017) 2

12. Chen, J., Wee, H.: Fully, (almost) tightly secure IBE and dual system groups. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part II. LNCS, vol. 8043, pp. 435–460. Springer, Heidelberg (Aug 2013) 2, 3, 5, 6
13. Chevallier-Mames, B., Joye, M.: A practical and tightly secure signature scheme without hash function. In: Abe, M. (ed.) CT-RSA 2007. LNCS, vol. 4377, pp. 339–356. Springer, Heidelberg (Feb 2007) 2
14. 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 (Apr / May 2002) 2, 5
15. Cramer, R., Shoup, V.: Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM J. Comput. 33(1), 167–226 (2003)
16. Escala, A., Herold, G., Kiltz, E., Ràfols, C., Villar, J.: An algebraic framework for Diffie-Hellman assumptions. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part II. LNCS, vol. 8043, pp. 129–147. Springer, Heidelberg (Aug 2013) 8, 9
17. Gay, R., Hofheinz, D., Kiltz, E., Wee, H.: Tightly CCA-secure encryption without pairings. In: Fischlin, M., Coron, J.S. (eds.) EUROCRYPT 2016, Part I. LNCS, vol. 9665, pp. 1–27. Springer, Heidelberg (May 2016) 1, 2, 3, 4, 5, 6, 9, 18, 19, 21
18. Gay, R., Hofheinz, D., Kohl, L., Pan, J.: More efficient (almost) tightly secure structure-preserving signatures. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018, Part II. LNCS, vol. 10821, pp. 230–258. Springer, Heidelberg (Apr / May 2018) 2, 3
19. Gentry, C.: Practical identity-based encryption without random oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445–464. Springer, Heidelberg (May / Jun 2006) 3
20. Giacon, F., Kiltz, E., Poettering, B.: Hybrid encryption in a multi-user setting, revisited. In: Abdalla, M., Dahab, R. (eds.) PKC 2018, Part I. LNCS, vol. 10769, pp. 159–189. Springer, Heidelberg (Mar 2018) 20
21. Gong, J., Chen, J., Dong, X., Cao, Z., Tang, S.: Extended nested dual system groups, revisited. In: Cheng, C.M., Chung, K.M., Persiano, G., Yang, B.Y. (eds.) PKC 2016, Part I. LNCS, vol. 9614, pp. 133–163. Springer, Heidelberg (Mar 2016) 2, 3
22. Gong, J., Dong, X., Chen, J., Cao, Z.: Efficient IBE with tight reduction to standard assumption in the multi-challenge setting. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part II. LNCS, vol. 10032, pp. 624–654. Springer, Heidelberg (Dec 2016) 2, 3, 6, 21, 22
23. Groth, J.: Simulation-sound NIZK proofs for a practical language and constant size group signatures. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 444–459. Springer, Heidelberg (Dec 2006) 3
24. Groth, J., Sahai, A.: Efficient noninteractive proof systems for bilinear groups. SIAM J. Comput. 41(5), 1193–1232 (2012) 3, 4
25. Han, S., Liu, S., Qin, B., Gu, D.: Tightly CCA-secure identity-based encryption with ciphertext pseudorandomness. Designs, Codes and Cryptography 86(3), 517–554 (Mar 2018), https://doi.org/10.1007/s10623-017-0339-3 3
26. Hesse, J., Hofheinz, D., Kohl, L.: On tightly secure non-interactive key exchange. In: Proc. CRYPTO 2018. Lecture Notes in Computer Science (2018) 2
27. Hofheinz, D.: Algebraic partitioning: Fully compact and (almost) tightly secure cryptography. In: Kushilevitz, E., Malkin, T. (eds.) TCC 2016-A, Part I. LNCS, vol. 9562, pp. 251–281. Springer, Heidelberg (Jan 2016) 1, 2

28. Hofheinz, D.: Adaptive partitioning. In: Coron, J., Nielsen, J.B. (eds.) EUROCRYPT 2017, Part III. LNCS, vol. 10212, pp. 489–518. Springer, Heidelberg (Apr / May 2017) 1
29. Hofheinz, D., Jager, T.: Tightly secure signatures and public-key encryption. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 590–607. Springer, Heidelberg (Aug 2012) 1, 2, 3
30. Hofheinz, D., Kiltz, E.: Secure hybrid encryption from weakened key encapsulation. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 553–571. Springer, Heidelberg (Aug 2007) 20
31. Hofheinz, D., Koch, J., Striecks, C.: Identity-based encryption with (almost) tight security in the multi-instance, multi-ciphertext setting. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 799–822. Springer, Heidelberg (Mar / Apr 2015) 2, 6
32. Jutla, C.S., Ohkubo, M., Roy, A.: Improved (almost) tightly-secure structure-preserving signatures. In: Abdalla, M., Dahab, R. (eds.) PKC 2018, Part II. LNCS, vol. 10770, pp. 123–152. Springer, Heidelberg (Mar 2018) 2
33. Jutla, C.S., Roy, A.: Shorter quasi-adaptive NIZK proofs for linear subspaces. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part I. LNCS, vol. 8269, pp. 1–20. Springer, Heidelberg (Dec 2013) 18
34. Kiltz, E., Wee, H.: Quasi-adaptive NIZK for linear subspaces revisited. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015, Part II. LNCS, vol. 9057, pp. 101–128. Springer, Heidelberg (Apr 2015) 18
35. Kurosawa, K., Desmedt, Y.: A new paradigm of hybrid encryption scheme. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 426–442. Springer, Heidelberg (Aug 2004) 2
36. Lewko, A.B., Waters, B.: Why proving HIBE systems secure is difficult. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 58–76. Springer, Heidelberg (May 2014) 2
37. Libert, B., Joye, M., Yung, M., Peters, T.: Concise multi-challenge CCA-secure encryption and signatures with almost tight security. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014, Part II. LNCS, vol. 8874, pp. 1–21. Springer, Heidelberg (Dec 2014) 1, 2
38. Libert, B., Peters, T., Joye, M., Yung, M.: Compactly hiding linear spans - tightly secure constant-size simulation-sound QA-NIZK proofs and applications. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015, Part I. LNCS, vol. 9452, pp. 681–707. Springer, Heidelberg (Nov / Dec 2015) 1
39. Morillo, P., Ràfols, C., Villar, J.L.: The kernel matrix Diffie-Hellman assumption. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part I. LNCS, vol. 10031, pp. 729–758. Springer, Heidelberg (Dec 2016) 8, 9
40. Naor, M., Reingold, O.: Number-theoretic constructions of efficient pseudo-random functions. In: 38th FOCS. pp. 458–467. IEEE Computer Society Press (Oct 1997) 21
41. Naor, M., Yung, M.: Public-key cryptosystems provably secure against chosen ciphertext attacks. In: 22nd ACM STOC. pp. 427–437. ACM Press (May 1990) 2, 5
42. Shoup, V., Shoup, V.: Why chosen ciphertext security matters. IBM Research Report RZ 3076 (1998) 2
43. Wang, Y., Matsuda, T., Hanaoka, G., Tanaka, K.: Memory lower bounds of reductions revisited. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018, Part I. LNCS, vol. 10820, pp. 61–90. Springer, Heidelberg (Apr / May 2018) 2