Identity-Based Encryption with Master Key-Dependent Message Security and Leakage-Resilience*

David Galindo[1], Javier Herranz[2], and Jorge Villar[2]

[1] University of Luxembourg
david.galindo@uni.lu
[2] Universitat Politècnica de Catalunya, Dept. Matemàtica Aplicada IV
{jherranz,jvillar}@ma4.upc.edu

Abstract. We introduce the concept of identity-based encryption (IBE) with master key-dependent chosen-plaintext (mKDM-sID-CPA) security. These are IBE schemes that remain secure even after the adversary sees encryptions, under some initially selected identities, of functions of the master secret keys. We then show that the Canetti, Halevi and Katz (Eurocrypt 2004) transformation delivers chosen-ciphertext secure key-dependent encryption (KDM-CCA) schemes when applied to mKDM-sID-CPA secure IBE schemes. Previously only one generic construction of KDM-CCA secure public key schemes was known, due to Camenisch, Chandran and Shoup (Eurocrypt 2009), and it required non-interactive zero knowledge proofs (NIZKs). Thus we show that NIZKs are not intrinsic to KDM-CCA public key encryption. As a proof of concept, we are able to instantiate our new concept under the Rank assumption on pairing groups and for affine functions of the secret keys. The scheme is inspired by the work by Boneh, Halevi, Hamburg and Ostrovsky (Crypto 2008). Our instantiation is only able to provide security against single encryption queries, or alternatively, against a *bounded* number of encryption queries. Secondly, we show that a special parameters setting of our main scheme provides master-key leakage-resilient identity-based encryption against chosen-plaintext attacks. This recently proposed security notion aims at taking into account security against side-channel attacks that only decrease the entropy of the master-key up to a certain threshold. Thirdly, we give new and better reductions between the Rank problem (previously named as Matrix-DDH or Matrix d-Linear problem) and the Decisional Linear problem.

1 Introduction

Master-Key Dependent Encryption. Until recently public key encryption (PKE) schemes were only required to provide confidentiality against adversaries

* Supported by the National Research Fund, Luxembourg C09/IS/04. Partially supported by the Spanish research project MTM2009-07694, and the European Commission through the ICT programme under contract ICT-2007-216676 ECRYPT II.

S. Foresti, M. Yung, and F. Martinelli (Eds.): ESORICS 2012, LNCS 7459, pp. 627–642, 2012.
© Springer-Verlag Berlin Heidelberg 2012

that see encryptions of plaintexts that depend solely on public information. That is, it was assumed (and even advocated) that an encryption scheme would never be used to encrypt its own decryption key. This requirement is certainly reasonable for many applications, but it has been challenged both by practical and foundational reasons [1,2]. The paradigmatic case is the scenario of *circular encryptions*, where for $n \geq 2$ public/secret key pairs $(pk_1, sk_1), \ldots, (pk_n, sk_n)$, the adversary is given the ciphertexts $Enc_{pk_1}(sk_2), Enc_{pk_2}(sk_3), \ldots, Enc_{pk_n}(sk_1)$, and still semantic security shall hold. Thus, a dedicated stronger security notion called *key-dependent message* security has emerged in the last few years [3]. Roughly speaking, it is required that semantic security holds even if the adversary sees encryptions of plaintexts that depend on the decryption keys. Such a scenario arises in systems that require hard-disk encryption, in computational soundness results in the area of formal methods, or in specific cryptographic protocols for anonymous credentials or fully homomorphic encryption. For the motivation, applications and history of key-dependent message security we refer to the excellent survey by Malkin, Teranishi and Yung [4].

The first breakthrough was due to Boneh, Halevi, Hamburg and Ostrovsky (BHHO) [5], who proposed a public key encryption scheme with indistinguishability against key-dependent chosen-plaintext attacks (KDM-CPA) in the standard model under the Decisional Diffie-Hellman assumption for affine functions of the secret key. Shortly after Applebaum, Cash, Peikert, and Sahai [6] proposed an efficient KDM-CPA secure scheme for affine functions under the Learning Parity with Noise assumption. Brakerski and Goldwasser [7] extended the BHHO scheme to a suite of KDM-CPA schemes secure under subgroup indistinguishability assumptions.

Camenisch, Chandran and Shoup [8] proposed a generic construction of chosen-ciphertext secure key-dependent encryption (KDM-CCA) schemes in the public key setting, that requires in particular a KDM-CPA secure scheme and specialized non-interactive zero knowledge proofs (NIZKs). By applying their transformation to (a variation of) the BHHO scheme, they obtained a KDM-CCA secure scheme under the Decision Linear assumption on pairing groups.

Master-Key Leakage-Resilient Identity-Based Encryption. Side channel attacks are often effective in recovering the secret key of cryptosystems that are provably secure otherwise [9,10]. On the other hand, it is desirable to extend the traditional provable security methodology to also include side channel attacks. This area of contemporary cryptography is usually referred to as *leakage-resilient cryptography* and it has been an increasingly active arena in recent years. Current security models assume an upper bound on the type or amount of information about the secret key that an adversary might learn from side-channel data. Here we allow the adversary to mount master-key leakage attacks, by allowing it to obtain the result of efficiently computable functions of the master-key. These functions might be asked adaptively, subject to the restriction that after all the queries the master-key has enough entropy left and that no master-key leakage queries are allowed after the adversary receives the challenge ciphertext. For the definitions of master-key leakage resilience we refer the reader to [11]. We

stress that in our case the adversary mounts a selective-identity chosen-plaintext attack with master-key leakage, that we denote as mIND-sID-LCPA. Let λ be the bit-length sum of the outputs obtained by the adversary via master-key leakage queries. λ is called the leakage parameter and it is assumed that $\lambda < L$, where L is the master-key length. The relative leakage (or leakage ratio) of the system is defined as λ/L.

Our Contribution. We initiate here the study of identity-based encryption (IBE) schemes secure against key dependent messages. This has a double interest, since IBE is relevant by itself [12] and by its numerous applications [13]. In IBE there are two types of secret keys, on the one hand a master secret key SK_i corresponding to the master public key PK_i; on the other hand the secret keys $sk[id]$ belonging to individual users id. This gives rise to two levels of key-dependent message security, depending on whether the adversary is allowed to ask for encryptions of functions of the master-keys or the user-keys. We choose here to deal only with master key-dependent messages (mKDM security). The first reason is that this allows us to update mKDM-sID-CPA to KDM-CCA. Secondly, in some cases master-key dependent security implies a restricted form of user-key dependent security "for free" (see Section 4.2 for the case of our scheme).

Informally, we say that an IBE scheme has master key-dependent indistinguishability against selective-identity and chosen plaintext attacks (mKDM-sID-CPA security for short) if no adversary is able to distinguish between encryptions of a particular message $\mathfrak{m}$ and encryptions of some functions of a set of master secret keys, under a certain set of identities chosen by the adversary ahead of time. We are able to give an instantiation of a mKDM-sID-CPA secure IBE in the standard model, under the Rank assumption over bilinear groups. The Rank assumption states that it is difficult to distinguish whether an $n \times n$ matrix has rank r_1 or r_2, where $2 \leq r_1 < r_2 \leq n$. As an additional contribution, which may be of independent interest, we give a new reduction between the Rank problem and the Decisional Linear problem. Our new reduction improves that of [14] from a linear to a logarithmic factor and can be used to improve the reduction from the Rank assumption to the Decisional Diffie-Hellman problem given in [5] in a similar fashion.

We also show that a slight modification of the new mKDM-sID-CPA secure IBE scheme maintains its security properties in the presence of leakage of parts of the master secret key. This implies, in particular, new chosen ciphertext secure public key encryption secure in the presence of leakage [14] which compare favourably with previous related work.

One of the most well-known applications of IBE in the theory of cryptography is the CHK generic construction of chosen-ciphertext secure public key encryption out of chosen-plaintext secure identity-based encryption. We show that the same transformation can be applied to the KDM setting, resulting in KDM-CCA secure public key encryption out of mKDM-sID-CPA secure identity-based encryption. Thus we show a practical generic construction for key-dependent chosen-ciphertext security that dispenses with the need of NIZKs from [8].

Plugging our concrete IBE scheme into the Canetti-Halevi-Katz transformation gives rise to a KDM-CCA secure encryption scheme under the Decisional Linear assumption. One drawback of our chosen-ciphertext secure schemes is that the public key size depends on the number of encryption queries per public key (but importantly ciphertext-size does not); in other words, we were only able to prove security against a *bounded* number of encryption queries per public key.

Concurrent and Independent Related Work. Concurrent work by Alperin-Sheriff and Peikert [15] deals with the related notion of user key-dependent message security. We stress that their IBE construction has a drawback similar to ours: therein, the size of the master public key, the user secret keys and the ciphertext depend on the parameter n, which is the maximum number of user secret keys involved in an encryption query. Also concurrently to this work, Hofheinz [16] has proposed a PKE scheme with KDM-CCA security in the standard model with compact ciphertexts. His construction is direct and does not use key-dependent IBE.

Organization. In Section 2 we recall previous KDM security notions for public key encryption. In Section 3 we define master key-dependent indistinguishability against selective-identity and chosen-plaintext attacks for identity-based encryption. We show then that the celebrated CHK transformation from passively-secure IBE to chosen-ciphertext PKE also holds in the KDM setting. Section 4 contains an instantiation of identity-based encryption with master key-dependent security in the standard model under the Decisional Linear assumption. Although we refer to the full version of this work [17] for the complete security proof, we include in this Section 4 a key part of it which may be of independent interest: a new and better relation between the Decisional Linear problem and the Rank problem. In Section 5 we discuss the leakage-resilience properties of (a slight variation of) our new IBE scheme. We end in Section 6 by outlining future research directions.

2 Preliminaries: KDM Secure Public Key Encryption

A public key encryption scheme Π supporting ciphertexts consists of four probabilistic polynomial algorithms, $\Pi = (\Pi.\mathsf{Stp}, \Pi.\mathsf{KG}, \Pi.\mathsf{Enc}, \Pi.\mathsf{Dec})$. The setup protocol $\Pi.\mathsf{Stp}$ takes as input a security parameter λ and outputs some public information pms, including plaintext space $\mathcal{M}$ and secret key space $\mathcal{S}$. The security parameter λ is included in the string pms, which is implicitly an input to the remaining algorithms. The key generation protocol $\Pi.\mathsf{KG}_{\mathsf{pms}}$ on input the empty string ε outputs a pair of secret and public keys, (sk, pk), where the secret key sk belongs to the set $\mathcal{S}$ of possible secret keys. The encryption protocol takes as input a public key pk and a message $m \in \mathcal{M}$ and outputs a ciphertext $C = \Pi.\mathsf{Enc}_{\mathsf{pms}}(pk, m)$. Finally, the decryption protocol takes as input secret key sk and a ciphertext C, and outputs $\widetilde{m} = \Pi.\mathsf{Dec}_{\mathsf{pms}}(sk, C)$, where $\widetilde{m} \in \mathcal{M} \cup \{\perp\}$. The correctness property requires that $\Pi.\mathsf{Dec}_{\mathsf{pms}}(sk, \Pi.\mathsf{Enc}_{\mathsf{pms}}(pk, m)) = m$, for any message $m \in \mathcal{M}$ and parameters pms generated by $\Pi.\mathsf{Stp}$ and any pair (sk, pk) generated by $\Pi.\mathsf{KG}_{\mathsf{pms}}$.

Informally, security with respect to key dependent messages under chosen plaintext attacks (KDM-CPA) requires that an adversary is not able to distinguish between encryptions of a particular message $\mathfrak{m}$ and encryptions of some functions (chosen by the adversary from a specific set of functions $\mathcal{F}$) of a set of secret keys. In the case of security with respect to key dependent messages under chosen ciphertext attacks (KDM-CCA), the adversary is given additional access to a decryption oracle that he can query for ciphertexts of his choice, as long as these ciphertexts are different to those the adversary has to distinghish.

For concrete security concerns, in the following definitions two integer parameters $n, q_e \geq 1$ are given as input to the security game, representing respectively the number of users in the system and the maximum number of encryption queries per user allowed to the adversary. To formalize this notion, we follow the definitions in [8,4]. Let $n, q_e \geq 1$ be integers and let $\mathcal{F} = \{f : \mathcal{S}^n \to \mathcal{M}\}$ be a finite set of efficiently computable functions. KDM-CPA security of a public key encryption scheme Π is defined with respect to the set of functions $\mathcal{F}$ through the following two experiments between a challenger and an adversary $\mathcal{A}_\Pi$. Let $\mathfrak{m} \in \mathcal{M}$ be a fixed message.

Experiment $\mathbf{ExpKDM\text{-}CCA}^{b,\Pi}_{\mathcal{A}_\Pi}(\lambda, n, q_e)$ is defined as follows, for $b = 0, 1$.

1. **Initialization.** The challenger runs $\mathsf{pms} \leftarrow \Pi.\mathsf{Stp}(\lambda)$ and then runs n times $(sk_i, pk_i) \leftarrow \Pi.\mathsf{KG}_{\mathsf{pms}}$ to produce n pairs $(sk_1, pk_1), \ldots, (sk_n, pk_n)$. The public keys $(pk_1, \ldots, pk_n)$ and pms are sent to $\mathcal{A}_\Pi$. A list L_{quer} is initially set to empty.
2. **Queries.** The adversary $\mathcal{A}_\Pi$ can adaptively make two types of queries to the challenger.
   (a) **Encryption queries.** For each $1 \leq i \leq n$ the adversary $\mathcal{A}_\Pi$ can make up to q_e encryption queries of the form (i, f) with $f \in \mathcal{F}$. The challenger computes $m = f(sk_1, \ldots, sk_n) \in \mathcal{M}$, and then sets $C = \Pi.\mathsf{Enc}_{\mathsf{pms}}(pk_i, m)$ in Experiment $b = 0$, and sets $C = \Pi.\mathsf{Enc}_{\mathsf{pms}}(pk_i, \mathfrak{m})$ in Experiment $b = 1$. The resulting ciphertext C is sent to $\mathcal{A}_\Pi$ and the tuple (i, C) is added to the list L_{quer}.
   (b) **Decryption queries.** $\mathcal{A}_\Pi$ can make a decryption query of the form (i, C), as long as $(i, C) \notin L_{\mathsf{quer}}$. The challenger sends back to $\mathcal{A}_\Pi$ the output $\Pi.\mathsf{Dec}_{\mathsf{pms}}(sk_i, C)$.
3. **Final guess.** The adversary $\mathcal{A}_\Pi$ outputs a bit $b' \in \{0, 1\}$.

Let us denote as Ω_b the event that $\mathcal{A}_\Pi$ outputs $b' = 1$ in Experiment $\mathbf{ExpKDM\text{-}CCA}^{b,\Pi}_{\mathcal{A}_\Pi}(\lambda, n, q_e)$. For any adversary $\mathcal{A}_\Pi$ as above let

$$\mathbf{AdvKDM\text{-}CCA}^{\Pi}_{\mathcal{A}_\Pi}(\lambda, n, q_e) = |\Pr[\Omega_0] - \Pr[\Omega_1]|$$

For any t, n, q_e we define the advantage function of the scheme Π for key-dependent message security against chosen-ciphertext attacks (KDM-CCA) as $\mathbf{AdvKDM\text{-}CCA}(\Pi, \lambda, n, q_e; t) = \max_{\mathcal{A}_\Pi} \left\{ \mathbf{AdvKDM\text{-}CCA}^{\Pi}_{\mathcal{A}_\Pi}(\lambda, n, q_e) \right\}$, where the maximum is over adversaries $\mathcal{A}_\Pi$ with time-complexity t and making no more than q_e encryption queries for each $1 \leq i \leq n$.

Definition 1. *A public key encryption scheme Π is polynomially-secure against key dependent chosen-ciphertext attacks with respect to the set of functions $\mathcal{F}$ if* $\mathbf{AdvKDM\text{-}CCA}(\Pi, \lambda, n, q_e; t)$ *is negligible in λ for all polynomial values of t, n, q_e.*

We refer to *security against single encryption queries* when $q_e = 1$, which means that the adversary can make several encryption queries but each one for a different public key. In this work we consider $\mathcal{F}$ to be the set of *affine functions*. This contains as particular cases constant functions (which lead to the notion of IND-CCA security in the multi-user setting [18]) and projections $f_i(sk_1, \ldots, sk_n) = sk_i$, for $1 \leq i \leq n$. An encryption scheme which is KDM-CCA-secure with respect to a set of functions containing projections achieves *clique security*, which in particular captures circular security.

3 From mKDM-sID-CPA Secure IBE to KDM-CCA Secure PKE

In this section we recall the Canetti-Halevi-Katz transformation [19] and show that it can be used to build IND-CCA encryption with key-dependent message security.

One-Time Signatures. We start by recalling the syntactic definition and security properties of one-time signatures. A (one-time) signature scheme $\Theta = (\Theta.\mathsf{Stp}, \Theta.\mathsf{KG}, \Theta.\mathsf{Sign}, \Theta.\mathsf{Vfy})$ consists of four probabilistic polynomial time algorithms. $\mathsf{pms}_\Theta \leftarrow \Theta.\mathsf{Stp}(1^\lambda)$ is the setup protocol, which produces some common public parameters (that will be an implicit input for the rest of protocols) for a given security parameter. $(sk_\Theta, vk_\Theta) \leftarrow \Theta.\mathsf{KG}()$ is the key generation protocol, which outputs a secret signing key sk_Θ and a public verification key vk_Θ. The signing protocol $\theta \leftarrow \Theta.\mathsf{Sign}(sk_\Theta, m)$ takes as input the signing key and a message m, and outputs a signature θ. Finally, the verification protocol $\{1, 0\} \leftarrow \Theta.\mathsf{Vfy}(vk_\Theta, m, \theta)$ takes as input the verification key, a message and a signature, and outputs 1 if the signature is valid, or 0 otherwise.

Regarding security, we consider an adversary F_Θ in the multi-user setting, with N users. F_Θ first receives N verification keys $\{vk_\Theta^{(i)}\}_{1 \leq i \leq N}$ obtained from running $\Theta.\mathsf{Stp}(1^\lambda) \rightarrow \mathsf{pms}_\Theta$ once and then running N times the protocol $\Theta.\mathsf{KG}() \rightarrow (sk_\Theta^{(i)}, vk_\Theta^{(i)})$, for $i = 1, \ldots, N$. The adversary can make at most one signature query of the form (i, m_i), for each $i = 1, \ldots, N$, for messages m_i of his choice, obtaining as answer valid signatures $\Theta.\mathsf{Sign}(sk_\Theta^{(i)}, m_i) \rightarrow \theta_i$. Finally F_Θ outputs a tuple $(i^\star, m^\star, \theta^\star)$. We say that the adversary F_Θ succeeds if $\Theta.\mathsf{Vfy}(vk_\Theta^{(i^\star)}, m^\star, \theta^\star) \rightarrow 1$ and $(m^\star, \theta^\star) \neq (m_{i^\star}, \theta_{i^\star})$.

We denote $\mathcal{F}_\Theta$'s success probability in the above game as $\mathbf{AdvOTS}^\Theta_{\mathcal{F}_\Theta}(\lambda, N)$. The signature scheme Θ is *one-time strongly unforgeable* if $\mathbf{AdvOTS}^\Theta_{\mathcal{F}_\Theta}(\lambda, N)$ is a negligible function of the security parameter $\lambda \in \mathbb{N}$, for any polynomial-time attacker $\mathcal{F}_\Theta$ against Θ and any polynomial value of N.

mKDM-sID-CPA Identity-Based Encryption. An identity-based encryption scheme Γ consists of five probabilistic polynomial algorithms,

$\Gamma = (\Gamma.\mathsf{Stp}, \Gamma.\mathsf{Mkg}, \Gamma.\mathsf{Ukg}, \Gamma.\mathsf{Enc}, \Gamma.\mathsf{Dec})$. The setup protocol, $\Gamma.\mathsf{Stp}$ takes as input a security parameter λ and outputs some system-wide parameters ibp to be shared by all the master authorities in the system. In particular, ibp includes the description of the sets of admissible identities, plaintexts and ciphertexts, $\mathcal{I}$, $\mathcal{M}$, $\mathcal{C}$ respectively. The string ibp is an implicit input to the remaining algorithms. $\Gamma.\mathsf{Mkg}_{\mathsf{ibp}}$ on input the empty string outputs (PK, SK), where PK is the master public key and SK is the master secret key. The user's key generation protocol, $\Gamma.\mathsf{Ukg}_{\mathsf{ibp}}$, on input the master secret key SK and an identity id, outputs the user's decryption key $sk[id]$. The encryption algorithm $\Gamma.\mathsf{Enc}_{\mathsf{ibp}}$ takes as input PK, an admissible identity id and a plaintext m and outputs a ciphertext $c = \Gamma.\mathsf{Enc}_{\mathsf{ibp}}(PK, id, m)$. Finally, the decryption protocol takes as input a decryption key $sk[id]$ and an admissible ciphertext c and outputs $\widetilde{m}$, where $\widetilde{m}$ is an admissible plaintext or the reject symbol $\perp$. The correctness property requires that $\Gamma.\mathsf{Dec}_{\mathsf{ibp}}(\Gamma.\mathsf{Ukg}(SK, id), \Gamma.\mathsf{Enc}_{\mathsf{ibp}}(PK, id, m)) = m$, for any identity $id \in \mathcal{I}$, message $m \in \mathcal{M}$, parameters ibp generated by $\Gamma.\mathsf{Stp}(1^k)$ and any pair (PK, SK) generated by $\Gamma.\mathsf{Mkg}_{\mathsf{ibp}}()$.

Informally, we say that an IBE scheme has master key-dependent indistinguishability against selective-identity and chosen plaintext attacks (mKDM-sID-CPA security, for short) if no adversary is able to distinguish between encryptions of a particular message $\mathfrak{m}$ and encryptions of some functions (chosen by the adversary from a specific set of functions $\mathcal{F}$) of a set of master secret keys.

We formalize next this notion. Let $n, q_e \geq 1$ be integers and let $\mathcal{F} = \{f : \mathcal{T}^n \to \mathcal{M}\}$ be a finite set of efficiently computable functions, where $\mathcal{T}$ is the set of master secret keys and $\mathcal{M}$ the set of admissible plaintexts. mKDM-sID-CPA security is defined with respect to the set of functions $\mathcal{F}$ through the following two experiments between a challenger and an adversary $\mathcal{A}_\Gamma$. Let $\mathfrak{m} \in \mathcal{M}$ be a fixed message.

Experiment $\mathbf{ExpKDM\text{-}sID\text{-}CPA}^{b,\Gamma}_{\mathcal{A}_\Gamma}(\lambda, n, q_e)$ is defined as follows, for $b = 0, 1$.

1. **Setup.** The challenger runs $\mathsf{ibp} \leftarrow \Gamma.\mathsf{Stp}(\lambda)$. The adversary $\mathcal{A}_\Gamma$ on input ibp outputs a tuple $\mathcal{I}^\star$ of $n \cdot q_e$ identities $\mathcal{I}^\star = (id_1^1, \ldots, id_1^{q_e}, \ldots, id_n^1, \ldots, id_n^{q_e})$.
2. **Initialization.** The challenger runs n times $\Gamma.\mathsf{Mkg}_{\mathsf{ibp}}$ to obtain n pairs $(PK_1, SK_1), \ldots, (PK_n, SK_n)$. The master public keys $(PK_1, \ldots, PK_n)$ are sent to $\mathcal{A}_\Gamma$.
3. **Queries.** The adversary $\mathcal{A}_\Gamma$ can adaptively make two types of queries to the challenger:

   (a) **Encryption Queries.** For every index i such that $1 \leq i \leq n$, a counter j is kept, with initial value $j = 1$. $\mathcal{A}_\Gamma$ can make encryption queries of the form (i, f), where $f \in \mathcal{F}$. The challenger computes $m = f(SK_1, \ldots, SK_n) \in \mathcal{M}$, and then sets $c = \Gamma.\mathsf{Enc}_{\mathsf{ibp}}(PK_i, id_i^j, m)$ when $b = 0$, and sets $c = \Gamma.\mathsf{Enc}_{\mathsf{ibp}}(PK_i, id_i^j, \mathfrak{m})$ if $b = 1$, where j is the current counter value. After the ciphertext c is sent to $\mathcal{A}_\Gamma$, the counter is updated as $j \leftarrow j + 1$. $\mathcal{A}_\Gamma$ can make up to q_e encryption queries per index i.

(b) **Private key Queries.** $\mathcal{A}_\Gamma$ can make users' private key queries of the form (i, id), where $1 \leq i \leq n$ and $id \neq id_i^j$ for all $j \in \{1, \ldots, q_e\}$. The challenger computes $sk_i[id] = \Gamma.\mathsf{Ukg}_{\mathsf{ibp}}(SK_i, id)$ and gives it back to $\mathcal{A}_\Gamma$.

4. **Final guess.** The adversary $\mathcal{A}_\Gamma$ outputs a bit $b' \in \{0, 1\}$.

Let us denote as Ω_b the event that $\mathcal{A}_\Gamma$ outputs $b' = 1$ in the above experiment. For any adversary $\mathcal{A}_\Gamma$ let $\mathbf{Adv\text{-}mKDM\text{-}sID\text{-}CPA}^{\Gamma}_{\mathcal{A}_\Gamma}(\lambda, n, q_e) = |\Pr[\Omega_0] - \Pr[\Omega_1]|$. For any t, n, q_e we define $\mathbf{Adv\text{-}mKDM\text{-}sID\text{-}CPA}(\Gamma, \lambda, n, q_e; t)$ as the quantity $\max_{\mathcal{A}_\Gamma} \left\{ \mathbf{Adv\text{-}mKDM\text{-}sID\text{-}CPA}^{\Gamma}_{\mathcal{A}_\Gamma}(\lambda, n, q_e) \right\}$, where the maximum is taken over adversaries $\mathcal{A}_\Gamma$ with time-complexity t.

Definition 2. *An identity-based encryption scheme Γ is secure against selective-identity and master key-dependent chosen plaintext attacks* (mKDM-sID-CPA) *with respect to the set of functions $\mathcal{F}$ if* $\mathbf{Adv\text{-}mKDM\text{-}sID\text{-}CPA}(\Gamma, \lambda, n, q_e; t)$ *is negligible in λ for polynomial values of n, t, q_e.*

Canetti-Halevi-Katz Transformation in the KDM Setting. Let $\Gamma = (\Gamma.\mathsf{Stp}, \Gamma.\mathsf{Mkg}, \Gamma.\mathsf{Ukg}, \Gamma.\mathsf{Enc}, \Gamma.\mathsf{Dec})$ be an IBE scheme and let $\Theta = (\Theta.\mathsf{KG}, \Theta.\mathsf{Sign}, \Theta.\mathsf{Vfy})$ be a one-time signature scheme. We use the well-known Canetti-Halevi-Katz transformation [19] to construct from these two primitives a public-key encryption scheme $\Pi = (\Pi.\mathsf{Stp}, \Pi.\mathsf{KG}, \Pi.\mathsf{Enc}, \Pi.\mathsf{Dec})$, as follows:

$\Pi.\mathsf{Stp}(1^\lambda)$: run $\mathsf{ibp} \leftarrow \Gamma.\mathsf{Stp}(1^\lambda)$ and $\mathsf{pms}_\Theta \leftarrow \Theta.\mathsf{Stp}(1^\lambda)$. We assume that verification keys output by Θ lie in the identities space of Γ. Define the output of the setup protocol as $\mathsf{pms} = (\mathsf{ibp}, \mathsf{pms}_\Theta)$.

$\Pi.\mathsf{KG}_{\mathsf{pms}}()$: parse $\mathsf{pms} = (\mathsf{ibp}, \mathsf{pms}_\Theta)$, run $(PK, SK) \leftarrow \Gamma.\mathsf{Mkg}_{\mathsf{ibp}}()$ and define the secret key as $sk = SK$ and the public key as $pk = PK$.

$\Pi.\mathsf{Enc}_{\mathsf{pms}}(pk, m)$: to encrypt a plaintext $m \in \mathcal{M}$ for a receiver with public key pk, parse $\mathsf{pms} = (\mathsf{ibp}, \mathsf{pms}_\Theta)$ and proceed as follows. Run $(sk_\Theta, vk_\Theta) \leftarrow \Theta.\mathsf{KG}()$ and set $id = vk_\Theta$; run $c \leftarrow \Gamma.\mathsf{Enc}_{\mathsf{ibp}}(pk, id, m)$; run $\theta \leftarrow \Theta.\mathsf{Sign}(sk_\Theta, c)$. The final ciphertext output by the algorithm is $C = (vk_\Theta, c, \theta)$.

$\Pi.\mathsf{Dec}_{\mathsf{pms}}(sk, C)$: parse $\mathsf{pms} = (\mathsf{ibp}, \Theta)$ and $C = (vk_\Theta, c, \theta)$. First of all, run $\Theta.\mathsf{Vfy}(vk_\Theta, c, \theta)$. If the output bit is 0, then stop and output $\perp$. Otherwise, set $id = vk_\Theta$ and run $sk[id] \leftarrow \Gamma.\mathsf{Ukg}_{\mathsf{ibp}}(sk, id)$ and output the result of running $\Gamma.\mathsf{Dec}_{\mathsf{ibp}}(sk[id], c)$.

Theorem 1. *If Γ enjoys* mKDM-sID-CPA *security with respect to a set of functions $\mathcal{F}$ and the signature scheme Θ is one-time strongly unforgeable, then the constructed public-key encryption scheme Π enjoys* KDM-CCA *security with respect to the same set of functions $\mathcal{F}$.*

The proof of this theorem, which is similar to that in [19], can be found in [17].

4 A New mKDM-sID-CPA Secure IBE Scheme for $q_e = 1$

In this section we propose an identity-based encryption scheme enjoying mKDM-sID-CPA security for $q_e = 1$. The new scheme upgrades the KDM-CPA techniques in [5] to the IBE setting.

4.1 Bilinear Pairings, Matrices and Hardness Assumptions

Let $\mathcal{G}$ be a group of prime order q admitting a bilinear pairing. That is, let $\mathcal{G}_T$ be a multiplicative group of prime order q and let $e(\cdot,\cdot) : \mathcal{G} \times \mathcal{G} \to \mathcal{G}_T$ an efficiently computable bilinear map. We will denote as $g_T = e(g,g)$ the generator of $\mathcal{G}_T$ induced by g a given generator of $\mathcal{G}$. Note that, due to the bilinear properties of the pairing, for any two integers $a, b \in \mathbb{Z}_q$ we have $g_T^{ab} = e(g^a, g^b) = e(g^a, g)^b = e(g^b, g)^a$.

These operations extend to vectors and matrices in a natural way. Let $\mathbb{Z}_q^{\ell_1 \times \ell_2}$ denote the set of all $\ell_1 \times \ell_2$ matrices and $\mathbb{Z}_q^{\ell_1 \times \ell_2; r}$ the matrices with rank r. In the special case of invertible matrices we will write $\mathrm{GL}_\ell(\mathbb{Z}_q) = \mathbb{Z}_q^{\ell \times \ell; \ell}$. Let $\mathcal{G}^{\ell_1 \times \ell_2}$ and ${\mathcal{G}_T}^{\ell_1 \times \ell_2}$ denote the set of all $\ell_1 \times \ell_2$ matrices over $\mathcal{G}$ and $\mathcal{G}_T$ respectively. Therefore, for any two matrices $\mathbf{A} \in \mathbb{Z}_q^{\ell_1 \times \ell_2}$ and $\mathbf{B} \in \mathbb{Z}_q^{\ell_2 \times \ell_3}$, we have $g^{\mathbf{AB}} = (g^{\mathbf{A}})^{\mathbf{B}} \in \mathcal{G}^{\ell_1 \times \ell_3}$. Again, we can naturally extend these definitions to matrices and bilinear pairings: if $\mathbf{A} \in \mathbb{Z}_q^{\ell_1 \times \ell_2}$ and $\mathbf{B} \in \mathbb{Z}_q^{\ell_2 \times \ell_3}$, then $e(g^{\mathbf{A}}, g^{\mathbf{B}}) = g_T^{\mathbf{AB}}$. Furthermore, if $\mathbf{C} \in \mathbb{Z}_q^{\ell_3 \times \ell_4}$, then it holds $g_T^{\mathbf{ABC}} = e(g^{\mathbf{AB}}, g^{\mathbf{C}}) = e(g^{\mathbf{A}}, g^{\mathbf{BC}}) \in {\mathcal{G}_T}^{\ell_1 \times \ell_4}$.

The security of our scheme will be reduced to the hardness of the Decisional Linear (DLin) problem [20]. The DLin problem consists in distinguishing between the distributions $(g, g^x, g^y, g^z, g^t, g^{(x^{-1}z + y^{-1}t)}) \in \mathcal{G}^6$ and $(g, g^x, g^y, g^z, g^t, g^u) \in \mathcal{G}^6$, where g is a generator of $\mathcal{G}$ and $x, y, z, t, u \in_{\mathrm{R}} \mathbb{Z}_q$ are chosen independently and at random. The problem is formally defined through the following two experiments between a challenger and a solver $\mathcal{A}_{\mathbf{DLin}}$. Experiment $\mathbf{ExpDLin}^b_{\mathcal{A}_{\mathbf{DLin}}}(\mathcal{G})$ is defined as follows, for $b = 0, 1$.

1. The challenger chooses a generator g of $\mathcal{G}$ and random $x, y, z, t, u \in_{\mathrm{R}} \mathbb{Z}_q$ independently and uniformly distributed.
   In Experiment $b = 0$, the challenger sends $(g, g^x, g^y, g^z, g^t, g^{(x^{-1}z + y^{-1}t)}) \in \mathcal{G}^6$ to $\mathcal{A}_{\mathbf{DLin}}$.
   In Experiment $b = 1$, it sends $(g, g^x, g^y, g^z, g^t, g^u) \in \mathcal{G}^6$ to $\mathcal{A}_{\mathbf{DLin}}$.
2. The solver $\mathcal{A}_{\mathbf{DLin}}$ outputs a bit $b' \in \{0, 1\}$.

Let us denote as Ω_b the event that $\mathcal{A}_{\mathbf{DLin}}$ outputs $b' = 1$ in Experiment $\mathbf{ExpDLin}^b_{\mathcal{A}_{\mathbf{DLin}}}(\mathcal{G})$. Let $\mathbf{AdvDLin}_{\mathcal{A}_{\mathbf{DLin}}}(\mathcal{G}) = |\Pr[\Omega_0] - \Pr[\Omega_1]|$. We can then define $\mathbf{AdvDLin}(\mathcal{G}; t) = \max_{\mathcal{A}_{\mathbf{DLin}}} \{\mathbf{AdvDLin}_{\mathcal{A}_{\mathbf{DLin}}}(\mathcal{G})\}$, where the maximum is taken over adversaries $\mathcal{A}_{\mathbf{DLin}}$ running in time at most t.

Definition 3. *The* Decisional Linear assumption *in $\mathcal{G}$ states that* $\mathbf{AdvDLin}(\mathcal{G}; t)$ *is negligible in $\lambda = \log |\mathcal{G}|$ for any value of t that is polynomial in λ.*

4.2 A mKDM-sID-CPA Secure Scheme

Let us consider the IBE scheme $\Gamma = (\Gamma.\mathsf{Stp}, \Gamma.\mathsf{Mkg}, \Gamma.\mathsf{Ukg}, \Gamma.\mathsf{Enc}, \Gamma.\mathsf{Dec})$ defined as follows:

$\Gamma.\mathsf{Stp}(1^\lambda)$*:* a pairing group $(\mathcal{G}, \mathcal{G}_T, e(\cdot,\cdot))$ of prime order q, where q is λ-bits long, and generators $g \in \mathcal{G}, g_T = e(g,g) \in \mathcal{G}_T$ are chosen. A second security parameter $\ell > 4\lambda$ is also considered. Therefore, we define $\mathsf{ibp} = (\lambda, \ell, q, \mathcal{G}, g, \mathcal{G}_T, g_T, e(\cdot,\cdot))$.

$\Gamma.\mathsf{Mkg}_{\mathsf{ibp}}()$*:* firstly, take $\mathbf{S} \in_{\mathrm{R}} \mathbb{Z}_q^{2\times\ell;2}$, $\widetilde{\mathbf{S}} \in_{\mathrm{R}} \mathbb{Z}_q^{\ell\times 2;2}$ and a binary vector $\boldsymbol{x} \in_{\mathrm{R}} \{0,1\}^{\ell\times 1}$, and compute $g_T^{\boldsymbol{y}} = g_T^{-\mathbf{S}\boldsymbol{x}} \in \mathcal{G}_T^{2\times 1}$. Then define the matrices $\mathbf{F}_{id}$ and $\widetilde{\mathbf{F}}_{id}$ for $id \in \mathbb{Z}_q$ as $\mathbf{F}_{id} = \mathbf{S}\mathbf{T}_{id} \in \mathbb{Z}_q^{2\times\ell}$ and $\widetilde{\mathbf{F}}_{id} = \mathbf{T}_{id}\widetilde{\mathbf{S}} \in \mathbb{Z}_q^{\ell\times 2}$, where $\mathbf{T}_{id} = \mathbf{T_0} + id\mathbf{T_1} \in \mathbb{Z}_q^{\ell\times\ell}$ is a random (matrix) polynomial of degree 1, with $\mathbf{T}_0 \in_{\mathrm{R}} \mathbb{Z}_q^{\ell\times\ell}$ and $\mathbf{T}_1 \in \mathrm{GL}_\ell(\mathbb{Z}_q)$. Note that it holds $\mathbf{F}_{id}\widetilde{\mathbf{S}} = \mathbf{S}\widetilde{\mathbf{F}}_{id}$ for any $id \in \mathbb{Z}_q$. The public and master secret keys are then $PK = (g^{\mathbf{S}}, g^{\widetilde{\mathbf{S}}}, g^{\mathbf{S}\mathbf{T_0}}, g^{\mathbf{S}\mathbf{T_1}}, g^{\mathbf{T_0}\widetilde{\mathbf{S}}}, g^{\mathbf{T_1}\widetilde{\mathbf{S}}}, g_T^{-\mathbf{S}\boldsymbol{x}})$ and $SK = g_T^{\boldsymbol{x}} \in \mathcal{G}_T^{\ell\times 1}$.

$\Gamma.\mathsf{Ukg}_{\mathsf{ibp}}(SK, id)$*:* for an identity $id \in \mathbb{Z}_q$ the secret key $sk[id] = (g^{\boldsymbol{d}_1}, g^{\boldsymbol{d}_2}) \in \mathcal{G}^{\ell\times 1} \times \mathcal{G}^{\ell\times 1}$ is generated as $g^{\boldsymbol{d}_1} = g^{\boldsymbol{x}} \cdot g^{\widetilde{\mathbf{F}}_{id}\boldsymbol{t}}$ and $g^{\boldsymbol{d}_2} = g^{\widetilde{\mathbf{S}}\boldsymbol{t}}$, where $\boldsymbol{t} \in_{\mathrm{R}} \mathbb{Z}_q^{2\times 1}$ and $g^{\boldsymbol{x}}$ is computed component-wise from $SK = g_T^{\boldsymbol{x}}$ (remember $\boldsymbol{x}$ is a binary vector). The user can verify the validity of $sk[id]$ by checking the equation $g_T^{-\mathbf{S}\boldsymbol{x}} \cdot e(g^{\mathbf{S}}, g^{\boldsymbol{d}_1}) = e(g^{\mathbf{F}_{id}}, g^{\boldsymbol{d}_2})$.

$\Gamma.\mathsf{Enc}_{\mathsf{ibp}}(PK, id, m)$*:* to encrypt a message $m \in \mathcal{G}_T$ for an identity id and master public key PK, a row vector $\boldsymbol{r} \in_{\mathrm{R}} \mathbb{Z}_q^{1\times 2}$ is chosen and the ciphertext $(g^{\boldsymbol{c}_1}, g^{\boldsymbol{c}_2}, c) \in \mathcal{G}^{1\times\ell} \times \mathcal{G}^{1\times\ell} \times \mathcal{G}_T$ is computed as $g^{\boldsymbol{c}_1} = g^{\boldsymbol{r}\mathbf{S}}$, $g^{\boldsymbol{c}_2} = g^{\boldsymbol{r}\mathbf{F}_{id}}$ and $c = g_T^{-\boldsymbol{r}\mathbf{S}\boldsymbol{x}} \cdot m$. The ciphertext fulfils the equation $e(g^{\boldsymbol{c}_1}, g^{\widetilde{\mathbf{F}}_{id}}) = e(g^{\boldsymbol{c}_2}, g^{\widetilde{\mathbf{S}}})$.

$\Gamma.\mathsf{Dec}_{\mathsf{ibp}}(sk[id], C)$*:* let $(g^{\boldsymbol{c}_1}, g^{\boldsymbol{c}_2}, c)$ be a ciphertext for an identity id. The user who owns $sk[id] = (g^{\boldsymbol{d}_1}, g^{\boldsymbol{d}_2})$ recovers $m = c \cdot e(g^{\boldsymbol{c}_1}, g^{\boldsymbol{d}_1})/e(g^{\boldsymbol{c}_2}, g^{\boldsymbol{d}_2})$.

A Simpler but Insecure Scheme. Notice that an extension of the Boneh *et al.* KDM-CPA scheme [5] *à la* Boneh and Boyen [21] leads to an insecure scheme, in the following sense. Let us consider the case where user-keys would have been of the form $sk[id] = (g^{\boldsymbol{d}_1}, g^{\boldsymbol{d}_2})$ with $g^{\boldsymbol{d}_1} = g^{\boldsymbol{x}} F_{id}^{\boldsymbol{t}}$ and $g^{\boldsymbol{d_2}} = g^{\boldsymbol{t}}$, where $\boldsymbol{t} \in_{\mathrm{R}} \mathbb{Z}_q^{\ell}$ and $F_{id} \in \mathcal{G}$ is defined as $F_{id} = T_0 T_1^{id}$ for $T_0, T_1 \in_{\mathrm{R}} \mathcal{G}$ (ciphertexts would be changed accordingly). In such a case, an adversary that obtains a single user-key $sk[id]$ can compute $e(g^{\boldsymbol{d}_1}, g) = g_T^{\boldsymbol{x}} \cdot e(F_{id}, g^{\boldsymbol{t}})$ on the one hand, and $e(F_{id}, g^{\boldsymbol{d}_2}) = e(F_{id}, g^{\boldsymbol{t}})$ on the other hand. The adversary thus recovers $g_T^{\boldsymbol{x}}$, which leads to the recovery of master secret key, since $\boldsymbol{x} \in \{0,1\}^{\ell}$. For this reason we are forced to "hide" $\boldsymbol{t}$ even more, by multiplying it with the matrix $\widetilde{\mathbf{S}} \in \mathrm{GL}_\ell(\mathbb{Z}_q)$. This makes scheme description and security proofs more intricate, for example because some care must be taken regarding the invertibility and the probability distribution of such matrices $\widetilde{\mathbf{S}} \in \mathrm{GL}_\ell(\mathbb{Z}_q)$, when master public keys are rerandomized.

Affine Functions. Let us define the set of affine functions $\mathcal{F} = \{f : \mathcal{T}^n \to \mathcal{G}_T\}$, where $\mathcal{T}$ is the set of master secret keys. Let $SK_1, \ldots, SK_n \in \mathcal{G}_T^{\ell}$ be n secret keys generated by $\Gamma.\mathsf{Ukg}_{\mathsf{ibp}}()$. Following the notation in [5], for every $n\ell$-vector $\boldsymbol{u} = (u_i)$ over $\mathbb{Z}_q$, every $n\ell$-vector $\boldsymbol{s} \in \mathcal{G}_T^{n\ell}$ and every scalar $H \in \mathcal{G}_T$, let $f_{\boldsymbol{u},H}(\boldsymbol{s}) = \prod_{i=1,\ldots,n\ell} g_T^{u_i} \cdot s_i + H \in \mathcal{G}_T$. Then, $\mathcal{F} = \{f_{\boldsymbol{u},H} : \mathcal{G}_T^{n\ell} \to \mathcal{G}\}_{\boldsymbol{u}\in\mathbb{Z}_q^{n\ell}, H\in\mathcal{G}_T}$.

Additionally, since the algorithm $\Gamma_0.\mathsf{Ukg}_{\mathsf{ibp}}(SK, id)$ can be seen as an affine function from $\mathcal{G}^{\ell}$ to $\mathcal{G}^{2\ell}$, we obtain uKDM-sID-CPA security [15] with respect to the set of affine functions from $\mathcal{G}^{2n\ell}$ to $\mathcal{G}_T$. Alas, this is is only a restricted form of uKDM-sID-CPA security, since in particular we can not encrypt the j-th selection function $(sk[id_1], \ldots, sk[id_n]) \mapsto sk[id_j]$, as $sk[id_j] \in \mathcal{G}^{2\ell}$.

4.3 mKDM-sID-CPA Security of Γ and KDM-CCA Secure Public Key Encryption

The scheme Γ is mKDM-sID-CPA secure with respect to the set of affine functions $\mathcal{F}$ and for $q_e = 1$ encryption queries per master public key, assuming the hardness of the Decisional Linear problem in the group $\mathcal{G}$. The proof of the following theorem, which is technically quite involved, can be found in [17]. In the latter reference it is also discussed how to extend this scheme to another IBE scheme that allows a predefined number of encryption queries $q_e >> 1$, with the downside that the master public key has length linear in q_e. A similar problem is encountered in the uKDM-sID-CPA IBE scheme from [15], where the efficiency of the scheme depends linearly in n, the number of participants involved in the security game.

Theorem 2. $\mathbf{Adv\text{-}mKDM\text{-}sID\text{-}CPA}(\Gamma, \lambda, \ell, n, 1; t) \leq$
$2(3n+4)2^{-\lambda} + 8\,(\lceil 1.71 \log_2 \ell \rceil + 1)\,\mathbf{AdvDLin}(\mathcal{G}; t')$.

Note that in our case the loss factor in the reduction is constant with respect to the number n of master keys. The factor only grows logarithmically on the security parameter ℓ. When the CHK transformation is applied to our IBE scheme together with Mohassel's one-time signature scheme [22], the resulting public key scheme achieves KDM-CCA security for $q_e = 1$, with a reduction loss factor that does not depend on n.

Although the result stated in Theorem 2 relates the KDM security of our scheme with the hardness of the Decisional Linear problem, the actual proof relates the security of the scheme with the hardness of a different problem, the Rank problem. The final result is obtained by applying a new and better relation between the Rank problem and the Decisional Linear problem, which may be of independent interest. The details are given in the following section.

4.4 The Rank Problem

We consider an assumption related to matrices. Given a (multiplicative) cyclic group $\mathcal{G}$ of prime order q, the $\mathbf{Rank}(\mathcal{G}, \ell_1, \ell_2, r, s)$ problem informally consists of distinguishing if a given matrix in $\mathbb{Z}_q^{\ell_1 \times \ell_2}$ has rank r or has rank s for given integers $r \neq s$, when the matrix is hidden in the exponent of a generator g of $\mathcal{G}$. The problem is formally defined through the following two experiments between a challenger and a distinguisher $\mathcal{A}_{\mathbf{Rank}}$. For $b = 0, 1$, experiment $\mathbf{ExpRank}^b_{\mathcal{A}_{\mathbf{Rank}}}(\mathcal{G}, \ell_1, \ell_2, r, s)$ is defined as follows.

1. In Experiment $b = 0$, the challenger chooses $\mathbf{M} \in_{\mathrm{R}} \mathbb{Z}_q^{\ell_1 \times \ell_2; r}$ and sends $g^{\mathbf{M}}$ to $\mathcal{A}_{\mathbf{Rank}}$.
   In Experiment $b = 1$, it chooses $\mathbf{M} \in_{\mathrm{R}} \mathbb{Z}_q^{\ell_1 \times \ell_2; s}$ and sends $g^{\mathbf{M}}$ to $\mathcal{A}_{\mathbf{Rank}}$.
2. The solver $\mathcal{A}_{\mathbf{Rank}}$ outputs a bit $b' \in \{0, 1\}$.

Let us denote as Ω_b the event that $\mathcal{A}_{\mathbf{Rank}}$ outputs $b' = 1$ in Experiment $\mathbf{ExpRank}^b_{\mathcal{A}_{\mathbf{Rank}}}(\mathcal{G}, \ell_1, \ell_2, r, s)$. For any such adversary $\mathcal{A}_{\mathbf{Rank}}$ let

$$\mathbf{AdvRank}_{\mathcal{A}_{\mathbf{Rank}}}(\mathcal{G}, \ell_1, \ell_2, r, s) = |\Pr[\Omega_0] - \Pr[\Omega_1]|$$

We can then define

$$\mathbf{AdvRank}(\mathcal{G}, \ell_1, \ell_2, r, s; t) = \max_{\mathcal{A}_{\mathbf{Rank}}} \{\mathbf{AdvRank}_{\mathcal{A}_{\mathbf{Rank}}}(\mathcal{G}, \ell_1, \ell_2, r, s)\},$$

where the maximum is taken over adversaries $\mathcal{A}_{\mathbf{Rank}}$ running in time at most t.

Definition 4. *The* $\mathbf{Rank}(\mathcal{G}, \ell_1, \ell_2, r, s)$ *assumption in a group* $\mathcal{G}$ *states that* $\mathbf{AdvRank}(\mathcal{G}, \ell_1, \ell_2, r, s; t)$ *is negligible in* $\lambda = \log |\mathcal{G}|$ *for any value of* t *that is polynomial in* λ.

The Rank assumption appeared in recent papers under the names Matrix-DDH [5] and Matrix d-Linear [14]. Therein, it was already proved that the Rank problem is harder than the Decisional Linear problem. However, the reduction given in the next proposition substantially improves the reductions previously given. Namely, the loss factor is no longer linear but logarithmic in the rank.

Proposition 1. *For any* ℓ_1, ℓ_2, r, s *such that* $2 \leq s < r \leq \min(\ell_1, \ell_2)$ *we have*

$$\begin{aligned}\mathbf{AdvRank}(\mathcal{G}, \ell_1, \ell_2, r, s; t) &\leq \left\lceil \tfrac{\log(3r) - \log(3s-2)}{\log 3 - \log 2} \right\rceil \mathbf{AdvDLin}(\mathcal{G}; t') \\ &\leq \lceil 1.71(\log_2 r - \log_2(s-1)) \rceil \, \mathbf{AdvDLin}(\mathcal{G}; t'),\end{aligned}$$

where $t' = t + \mathcal{O}(\ell_1 \ell_2 (\ell_1 + \ell_2))$, *taking the cost of an exponentiation in* $\mathcal{G}$ *as one time unit.*

Before proving the proposition, we note that the $\mathbf{Rank}(\mathcal{G}, \ell_1, \ell_2, r, s)$ problem is random self-reducible, because given $\mathbf{M}_0 \in \mathbb{Z}_q^{\ell_1 \times \ell_2; k}$, for random $\mathbf{L} \in_{\mathrm{R}} \mathrm{GL}_{\ell_1}(\mathbb{Z}_q)$ and $\mathbf{R} \in_{\mathrm{R}} \mathrm{GL}_{\ell_2}(\mathbb{Z}_q)$ the product $\mathbf{L}\mathbf{M}_0\mathbf{R}$ is uniformly distributed in $\mathbb{Z}_q^{\ell_1 \times \ell_2; k}$. For the actual proof of Proposition 1, we use the following result.

Lemma 1. *Any distinguisher for* $\mathbf{Rank}(\mathcal{G}, \ell_1, \ell_2, k - \delta, k)$, $\ell_1, \ell_2 \geq 3$, $k \geq 3$, $1 \leq \delta \leq \lfloor \frac{k}{3} \rfloor$ *can be converted into a distinguisher for the Decisional Linear* (DLin) *problem, with the same advantage and running essentially within the same time.*

Proof. We will use the notation $\mathbf{A} \oplus \mathbf{B}$ for block matrix concatenation:

$$\mathbf{A} \oplus \mathbf{B} = \left(\begin{array}{c|c} \mathbf{A} & 0 \\ \hline 0 & \mathbf{B} \end{array}\right)$$

In addition, we will denote I_ℓ and $0_{\ell_1 \times \ell_2}$ for the neutral element in $\mathrm{GL}_\ell(\mathbb{Z}_q)$ and the null matrix in $\mathbb{Z}_q^{\ell_1 \times \ell_2}$, respectively. Given the DLin instance $(g, g^x, g^y, g^z, g^t, g^u)$ the DLin distinguisher builds the $\ell_1 \times \ell_2$ matrix

$$\mathbf{M} = \underbrace{\begin{pmatrix} x & 0 & 1 \\ 0 & y & t \\ z & 1 & u \end{pmatrix} \oplus \cdots \oplus \begin{pmatrix} x & 0 & 1 \\ 0 & y & t \\ z & 1 & u \end{pmatrix}}_{\delta \text{ times}} \oplus I_{k-3\delta} \oplus 0_{(\ell_1 - k) \times (\ell_2 - k)}$$

and submits the randomized matrix $g^{\mathbf{LMR}}$ to the $\mathbf{Rank}(\mathcal{G}, \ell_1, \ell_2, k - \delta, k)$ distinguisher, where $\mathbf{L} \in_{\mathrm{R}} \mathrm{GL}_{\ell_1}(\mathbb{Z}_q)$ and $\mathbf{R} \in_{\mathrm{R}} \mathrm{GL}_{\ell_2}(\mathbb{Z}_q)$. Notice that if $u = x^{-1}z + y^{-1}t \mod q$ then the resulting matrix is a random matrix in $\mathcal{G}^{\ell_1 \times \ell_2; k-\delta}$. Otherwise, it is a random matrix in $\mathcal{G}^{\ell_1 \times \ell_2; k}$. □

We can now apply a hybrid argument to prove Proposition 1. Let us consider the sequence of integers $\{r_i\}$ defined by the recurrence $r_0 = s$ and $r_{i+1} = \lfloor \frac{3r_i}{2} \rfloor$, and let k be the smallest index such that $r_k \geq r$. Then define a sequence of random matrices $\{\mathbf{M}_i\}$, where $\mathbf{M}_i \in_{\mathrm{R}} \mathbb{Z}_q^{\ell_1 \times \ell_2; r_i}$ for $i = 0, \ldots, k-1$, and $\mathbf{M}_k \in_{\mathrm{R}} \mathbb{Z}_q^{\ell_1 \times \ell_2; r}$. For any distinguisher $\mathcal{A}_{\mathbf{Rank}}$ with running time upper bounded by t, let $p_i = \Pr[1 \leftarrow \mathcal{A}_{\mathbf{Rank}}(g^{\mathbf{M}_i})]$. By Lemma 1, we have that for $i = 0, \ldots, k-2$

$$|p_{i+1} - p_i| = \mathbf{AdvRank}_{\mathcal{A}_{\mathbf{Rank}}}(\mathcal{G}, \ell_1, \ell_2, r_{i+1}, r_i) \leq \mathbf{AdvDLin}(\mathcal{G}; t'),$$
$$|p_k - p_{k-1}| = \mathbf{AdvRank}_{\mathcal{A}_{\mathbf{Rank}}}(\mathcal{G}, \ell_1, \ell_2, r, r_{k-1}) \leq \mathbf{AdvDLin}(\mathcal{G}; t')$$

Therefore, $\mathbf{AdvRank}_{\mathcal{A}_{\mathbf{Rank}}}(\mathcal{G}, \ell_1, \ell_2, r, s) = |p_k - p_0| \leq$
$|p_1 - p_0| + \ldots + |p_k - p_{k-1}| \leq k \cdot \mathbf{AdvDLin}(\mathcal{G}; t')$.
On the other hand, since $\lfloor \frac{3x}{2} \rfloor \geq \frac{3x-1}{2}$ then $r_k \geq \left(\frac{3}{2}\right)^k \left(s - \frac{2}{3}\right)$, which implies that $k \leq \frac{\log(3r) - \log(3s-2)}{\log 3 - \log 2}$. □

In [17] we prove this same relation between the Rank problem and another computational problem, the Decisional 3-Party Diffie-Hellman (D3DH) problem [23,24,25]. As a consequence, the mKDM-CPA security of our scheme may rely on either the Decisional Linear assumption or the Decisional 3-Party Diffie-Hellman assumption.

5 Leakage-Resilient Identity-Based Encryption and Applications

The Boneh *et al.* KDM-CPA secure PKE scheme [5] was shown to be resilient against a leakage of up to $L(1 - o(1))$ bits of the secret key under a suitable parameters selection by Naor and Segev [14]. Similar results have been proven for other extensions of Boneh *et al.* scheme, notably in [6,7]. We show that this is also the case for our scheme by slightly changing the parameters. More precisely, an improved parameters setting of our mKDM-sID-CPA scheme provides master-key leakage resilience in the relative leakage model [11], with leakage ratio $1 - o(1)$, under the Decisional Linear assumption. Such a property is particularly useful, since IBE schemes that are secure against master-key leakage resilient and selective-identity chosen-plaintext attacks imply chosen ciphertext secure public key encryption secure in the presence of leakage [14].

Some Technical Tools. To give an intuition on why our scheme is leakage-resilient we need to recall some technical tools.

Definition 5 (Min-entropy). *The min-entropy of a random variable X is defined as $\mathcal{H}_\infty(X) = -\log(\max_x \Pr[X = x])$.*

Intuitively, the min-entropy of a random variable measures the difficulty of any adversary, even unbounded, to predict the value of the variable. The notion that measures how hard is predicting X given knowledge of another random variable Y is that of average min-entropy.

Definition 6 (Average min-entropy). *The average min-entropy of X given Y is defined as* $\mathcal{H}_\infty(X|Y) = -\log\left(\mathbb{E}_{y\leftarrow Y}\left[\max_x \Pr[X=x|Y=y]\right]\right)$.

Definition 7 (Statistical distance). *The statistical distance between two random variables X, Y over a finite set Ω is defined as*

$$\mathcal{D}(X,Y) = \frac{1}{2}\sum_{\omega\in\Omega} |\Pr[X=\omega] - \Pr[Y=\omega]|$$

Lemma 2 ([26] adapted). *Let A, B be random variables such that $\mathcal{H}_\infty(A|B) \geq h$. Let $\mathcal{H} = \{H_{\boldsymbol{v}} : \mathbb{Z}_q^\ell \to \mathbb{Z}_q\}_{\boldsymbol{v}\in\mathbb{Z}_q^\ell}$ be the family of universal hash functions $\boldsymbol{x} \mapsto \boldsymbol{v}\boldsymbol{x}$. Let V be the uniform distribution in $\mathbb{Z}_q^\ell$. If $\log q \leq h - 2t$ holds, then $\mathcal{D}\left((H_V(A), V, B), (U_{\mathbb{Z}_q}, V, B)\right) \leq 2^{-t}$.*

For the definitions of master-key leakage resilience we refer the reader to [11]. For our current exposition it suffices to say that we are considering an standard IND-sID-CPA adversary which is allowed to decrease the min-entropy of the master-key by a given number of bits *before the challenge ciphertext is known*. We refer to our leakage security notion as IND-sID-LCPA (where L stands for leakage attacks).

Scheme and Master-Leakage Resilience. The modified IBE scheme $\Gamma' = (\mathsf{Stp}, \mathsf{Mkg}, \mathsf{Ukg}, \mathsf{Enc}, \mathsf{Dec})$ is obtained by only changing the set from which the master secret key SK is chosen. Instead of choosing $\boldsymbol{x} \in_{\mathrm{R}} \mathbb{Z}_2^\ell$ in $\Gamma.\mathsf{Mkg}$ from Section 4.2, the scheme Γ' chooses $\boldsymbol{x} \in_{\mathrm{R}} \mathbb{Z}_q^\ell$.

Note that the average min-entropy of the master secret key $\boldsymbol{x}$ given the public key and λ bits of leakage is $h = \ell\log q - 2\log q - \lambda$. Let us set $\ell = 3 + \frac{\lambda+2t}{\log q}$. Then Lemma 2 guarantees that $g_T^{-\boldsymbol{v}\boldsymbol{x}} \in \mathcal{G}_T$ is $\frac{1}{2^t}$-statistically close to the uniform distribution in $\mathcal{G}_T$. This turns out to be enough for proving mIND-sID-LCPA security, since in the simulation the legitimate ciphertext $(g^{\boldsymbol{r}\mathbf{S}}, g^{\boldsymbol{r}\mathbf{F}_{id}}, g_T^{-\boldsymbol{r}\mathbf{S}\boldsymbol{x}}\cdot m_\beta)$ is replaced by the illegitimate ciphertext $(g^{\boldsymbol{v}}, g^{\boldsymbol{v}\mathbf{T}_{id}}, g_T^{-\boldsymbol{v}\boldsymbol{x}}\cdot m_\beta)$ with $\boldsymbol{v} \in_{\mathrm{R}} \mathbb{Z}_q^\ell$, and the adversary can not tell the difference thanks to the Decision Linear assumption. Finally, the adversary will not be able to tell the difference (information-theoretically) between an encryption of m_0 or m_1 because thanks to Lemma 2 $g_T^{-\boldsymbol{v}\boldsymbol{x}} \in \mathcal{G}_T$ is statistically close to uniform.

We briefly comment on efficiency. For instance, for $\ell = 6$ our IBE scheme offers master-key leakage-resilience against $\frac{1}{2} - o(1)$ leakage ratio. In this case the ciphertext consists of 12 elements in $\mathcal{G}$ and 1 element in $\mathcal{G}_T$. By using the CHK transformation we obtain chosen-ciphertext leakage security under DLIN with leakage ratio $\frac{1}{2} - o(1)$ and ciphertext consisting of 18 elements in $\mathcal{G}$ and 1 element in $\mathcal{G}_T$. This compares favourably with existing schemes in the relative-leakage model.

Let us point out that via the IBE-to-signatures transformation, where messages to be signed play the role of identities, existentially unforgeable signature schemes can be obtained. Thus we only need to provide a full-identity secure variant of our master-leakage resilient scheme to obtain existentially unforgeable

signature schemes secure against $1-o(1)$ leakage-ratio under the Decisional Linear assumption. One possibility is to use a random oracle H to construct the elements $\mathbf{F}_{H(m)}$ and $\widetilde{\mathbf{F}}_{H(m)}$. Alternatively, we can use a matrix-based analogue of Waters' hash function [27] to implement $H(m)$; in this way, and at the cost of increasing the size of the public key of the signer, we obtain existentially unforgeable signature schemes secure against $1-o(1)$ leakage-ratio in the standard model under the Decisional Linear assumption.

6 Open Problems

Given the current state of the art ([15] and this work), the most prominent open problem is to build mKDM-sID-CPA secure IBE schemes for $q_e, n \geq 1$ where the master public key and ciphertext sizes do not depend on the number of challenge queries q_e nor on the number of users n. Another interesting research direction is to build efficient mKDM-sID-CPA secure IBE schemes from lattices, which would lead to the first lattice-based KDM-CCA secure public key encryption schemes.

References

1. Abadi, M., Rogaway, P.: Reconciling two views of cryptography (the computational soundness of formal encryption). J. Cryptology 15(2), 103–127 (2002)
2. Camenisch, J.L., Lysyanskaya, A.: An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 93–118. Springer, Heidelberg (2001)
3. Black, J., Rogaway, P., Shrimpton, T.: Encryption-Scheme Security in the Presence of Key-Dependent Messages. In: Nyberg, K., Heys, H.M. (eds.) SAC 2002. LNCS, vol. 2595, pp. 62–75. Springer, Heidelberg (2003)
4. Malkin, T., Teranishi, I., Yung, M.: Efficient Circuit-Size Independent Public Key Encryption with KDM Security. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 507–526. Springer, Heidelberg (2011)
5. Boneh, D., Halevi, S., Hamburg, M., Ostrovsky, R.: Circular-Secure Encryption from Decision Diffie-Hellman. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 108–125. Springer, Heidelberg (2008)
6. Applebaum, B., Cash, D., Peikert, C., Sahai, A.: Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 595–618. Springer, Heidelberg (2009)
7. Brakerski, Z., Goldwasser, S.: Circular and Leakage Resilient Public-Key Encryption under Subgroup Indistinguishability. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 1–20. Springer, Heidelberg (2010)
8. Camenisch, J., Chandran, N., Shoup, V.: A Public Key Encryption Scheme Secure against Key Dependent Chosen Plaintext and Adaptive Chosen Ciphertext Attacks. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 351–368. Springer, Heidelberg (2009)
9. Kocher, P.C.: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 104–113. Springer, Heidelberg (1996)

10. Kocher, P.C., Jaffe, J., Jun, B.: Differential Power Analysis. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999)
11. Lewko, A., Rouselakis, Y., Waters, B.: Achieving Leakage Resilience through Dual System Encryption. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 70–88. Springer, Heidelberg (2011)
12. Shamir, A.: Identity-Based Cryptosystems and Signature Schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)
13. Boneh, D., Franklin, M.: Identity-Based Encryption from the Weil Pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)
14. Naor, M., Segev, G.: Public-Key Cryptosystems Resilient to Key Leakage. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 18–35. Springer, Heidelberg (2009)
15. Alperin-Sheriff, J., Peikert, C.: Circular and KDM Security for Identity-Based Encryption. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 334–352. Springer, Heidelberg (2012)
16. Hofheinz, D.: Circular chosen-ciphertext security with compact ciphertexts. Cryptology ePrint Archive, Report 2012/150 (2012), `http://eprint.iacr.org/`
17. Galindo, D., Herranz, J., Villar, J.: Identity-based encryption with master key-dependent message security and applications. Cryptology ePrint Archive, Report 2012/142 (2012), `http://eprint.iacr.org/`
18. 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 (2000)
19. Canetti, R., Halevi, S., Katz, J.: Chosen-ciphertext security from identity-based encryption. In: [28], pp. 207–222
20. Boneh, D., Boyen, X., Shacham, H.: Short Group Signatures. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer, Heidelberg (2004)
21. Boneh, D., Boyen, X.: Efficient selective-id secure identity-based encryption without random oracles. In: [28], pp. 223–238
22. Mohassel, P.: One-Time Signatures and Chameleon Hash Functions. In: Biryukov, A., Gong, G., Stinson, D.R. (eds.) SAC 2010. LNCS, vol. 6544, pp. 302–319. Springer, Heidelberg (2011)
23. Laguillaumie, F., Paillier, P., Vergnaud, D.: Universally Convertible Directed Signatures. In: Roy, B. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 682–701. Springer, Heidelberg (2005)
24. Boneh, D., Sahai, A., Waters, B.: Fully Collusion Resistant Traitor Tracing with Short Ciphertexts and Private Keys. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 573–592. Springer, Heidelberg (2006)
25. Green, M., Hohenberger, S.: Practical Adaptive Oblivious Transfer from Simple Assumptions. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 347–363. Springer, Heidelberg (2011)
26. Dodis, Y., Ostrovsky, R., Reyzin, L., Smith, A.: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. SIAM J. Comput. 38(1), 97–139 (2008)
27. Waters, B.: Efficient Identity-Based Encryption Without Random Oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005)
28. Cachin, C., Camenisch, J.L. (eds.): EUROCRYPT 2004. LNCS, vol. 3027. Springer, Heidelberg (2004)