KDM-CCA Security from RKA Secure Authenticated Encryption *

Xianhui Lu[1,2], Bao Li[1,2], Dingding Jia[1,2]

1. Data Assurance and Communication Security Research Center,
Chinese Academy of Sciences, Beijing, 10093
2. State Key Laboratory of Information Security,
Institute of Information Engineering,
Chinese Academy of Sciences, Beijing, 100093
xhlu@is.ac.cn, lb@is.ac.cn, ddj@is.ac.cn

Abstract. We propose an efficient public key encryption scheme which is key-dependent message secure against chosen ciphertext attacks (KDM-CCA) with respect to affine functions based on the decisional composite residuosity assumption. Technically, we achieve KDM-CCA security by enhancing a chosen ciphertext secure scheme based on the high entropy hash proof system with three tools: a key-dependent message encoding, an entropy filter and an authenticated encryption secure against related-key attacks.

Keywords: public key encryption, key-dependent message security, related key attack, authenticated encryption.

1 Introduction

An encryption scheme is key-dependent message (KDM) secure if it is secure even when the adversary can access encryptions of messages that depend on the secret key. Due to its extensive usefulness in cryptographic protocol design and analysis [23, 16], hard disk encryption[19] and fully homomorphic public key encryption [28], KDM security was widely studied in recent years [32, 7, 34, 19, 4, 31, 20, 11, 40, 21, 8, 3, 2, 17].

Although the construction of KDM secure schemes in the random oracle model is very easy [23, 16, 6], in the standard model it remained an open problem until Boneh *et al.* [19] proposed the first construction. The main idea of Boneh *et al.*'s scheme is to construct key-dependent encryptions without knowing the private key. When considering the case of KDM-CCA, unfortunately, Boneh *et al.*'s approach causes a direct attack: an adversary can construct an encryption of the private key, submit it to the decryption oracle and obtain the private key.

* Supported by the National Basic Research Program of China (973 project, No.2014CB340603) and the National Nature Science Foundation of China (No.61379137, No.61272534).

Since the plaintexts may depend on the private key, existing techniques to achieve IND-CCA2 (Indistinguishability security against adaptive chosen ciphertext attacks) security in the standard model can not be used to construct KDM-CCA secure schemes directly. Camenisch, Chandran and Shoup [22] modified the Naor-Yung double encryption paradigm [41], and showed that one can combine a KDM-CPA (Key-dependent message security against chosen plaintext attacks) secure scheme with an IND-CCA2 secure scheme, along with an appropriate non-interactive zero-knowledge (NIZK) proof, to obtain a KDM-CCA secure scheme.

To construct practical KDM-CCA secure public key encryption (PKE) schemes, a direct solution is to replace the generic inefficient NIZK proof system by the hash proof system in [25]. Unfortunately, when the adversary can get encryptions of the private key of the hash proof system, the entropy of the private key will be leaked completely. To solve this problem, Hofheinz [33] proposed a "twice encryption" construction, in which the algorithm of the hash proof system shares the same private key with the encryption algorithm and two random coins are used: one for encryption and the other for hash proof. To prevent the adversary from generating valid ciphertexts of key-dependent messages, Hofheinz [33] added an authentication tag, constructed by embedding the plaintext into an encrypted LAF (Lossy Algebraic Filter), to the ciphertext. It guarantees that, in order to place a valid key-dependent decryption query, the adversary would have to guess the whole private key.

Galindo *et al.* [27] proposed a master key-dependent message (MKDM) secure IBE (Identity Based Encryption) scheme. Using the IBE to PKE transformation of Canetti, Halevi and Katz [24], they get a KDM-CCA secure PKE scheme. However, their concrete construction only achieves a bounded version of KDM security, that is, the adversary can only make a bounded number of encryption queries per public key.

1.1 Our Contribution

We propose an efficient KDM-CCA secure public key encryption scheme with respect to affine functions by enhancing an IND-CCA2 secure hybrid encryption scheme based on the high entropy hash proof system which was proposed by Kiltz *et al.* in [37]. Briefly, Kiltz *et al.* [37] provided a transformation from a k-entropic to a universal$_2$ hash proof system. Combining the latter with an AE-OT (Semantic and integrity security against one-time attack) secure data encapsulation mechanism (DEM) gives an IND-CCA2 secure hybrid encryption scheme. However, when key-dependent messages are encrypted by this hybrid encryption, the entropy of the private key of the hash proof system may be leaked completely.

Specifically, let $(u, e = \mathrm{DEM.E}_k(m))$ be a ciphertext of such a hybrid encryption scheme, where $(u, k) = \mathrm{KEM.E}_{pk}(r)$, KEM is the key encapsulation mechanism (KEM) constructed based on the hash proof system, pk is the public key, k is the encapsulated key. When key-dependent messages are encrypted by

this hybrid encryption, for example $e = \text{DEM.E}_k(f(sk))$ (sk denotes the private key of the KEM, $f(\cdot)$ denotes the key-dependent function), the entropy of the private key of the hash proof system may be leaked completely. To achieve KDM-CCA security, we enhance the hybrid encryption as follows:

- **Key-dependent message encoding.** To deal with the problem of entropy leakage of key-dependent encryptions, we enhance the hybrid encryption by using a key-dependent message encoding $\mathcal{E}(\cdot)$. Specifically, instead of direct encryption, the plaintexts are encoded as $\mathcal{E}(m)$ before encryption. We require that, $\mathcal{E}(f(sk))$ can be constructed publicly without using the private key sk. Hence $\text{DEM.E}_k(\mathcal{E}(f(sk)))$ will not leak any entropy of sk. In fact most of the KDM-CPA secure public key encryption schemes [19, 4, 20, 40] meet this requirement.
- **Entropy filter.** Although the key-dependent message encoding prevents the challenge ciphertexts from releasing the entropy of the private key of the hash proof system, it enables the adversary to construct valid key-dependent encryptions at the same time. Inspired by the technique of Hofheinz [33], we solve this problem by adding an authentication tag to the ciphertext. Specifically, we divide the entropy of the private key of the hash proof system into two parts, and use an entropy filter to derive the first part to construct an authentication tag. Let $\theta(\cdot)$ be an entropy filter, the DEM part of the hybrid encryption is enhanced as $\text{DEM.E}_k(\theta(m), \mathcal{E}(m))$.
- **RKA secure authenticated encryption.** To guarantee that authentication tag $\theta(m)$ can be used to prevent the adversary from constructing valid ciphertexts, we must prevent the challenge ciphertexts from releasing the entropy of the private key of the hash proof system derived by the entropy filter. The main difficulty is that, to prevent the entropy leakage, the challenger needs to provide a random encapsulated key for each key-dependent encryption query. However, the entropy of the second part of the hash proof system is not enough to protect the encapsulated keys for all of the key-dependent encryption queries. We solve this problem by using an RKA secure authenticated encryption. Specifically, let k^* be an original key for the RKA secure authenticated encryption scheme, in the construction of challenge ciphertexts, the keys for the authenticated encryption are affine functions of k^*. And k^* is hidden from the adversary perfectly by using linearly dependent combinations of the second part of the private key. According to the definition of RKA security, the encryption scheme is secure if k^* is randomly distributed. Therefor, we can hide the authentication tag from the adversary perfectly.

On RKA Secure Authenticated Encryption. Related-key attacks (RKAs) were first proposed in [38, 14] as a cryptanalysis tool for block ciphers. Motivated by real attacks [15, 18], theoretical model for RKA was proposed by Bellare and Kohno [12]. In the last decade the RKA security for a wide range of cryptographic primitives was studied [9, 13, 5, 10, 29, 30, 43, 36, 35, 39, 1].

Up to now the RKA security for authenticated encryption has not been studied yet. We propose formal definition for the semantic security and integrity security of authenticated encryption under RKAs. Similar to [12], we consider RKA security with respect to a class of related-key deriving (RKD) functions F which specify the key-relations available to the adversary. Informally, we let the adversary apply chosen plaintext attacks and forgery attacks with respect to a set of keys $k_1, \cdots, k_l$ which are derived from the original key k via a known function $f \in F$.

According to the framework in [10], it is easy to transform an AE-OT secure authenticated encryption scheme to an RKA secure authenticated encryption scheme based a RKA secure PRF (Pseudorandom function). Although the recent construction of RKA secure PRF with respect to affine function in [1] seems very efficient in general case, it will be very inefficient for our application. Specifically, the RKA secure PRF proposed by Abdalla *et al.* in [1] can be described as follows:

$$\mathrm{F}(\boldsymbol{a}, x) = \mathrm{NR}^*(\boldsymbol{a}, 11||\mathrm{h}(x, (g^{\boldsymbol{a}[1]}, \cdots, g^{\boldsymbol{a}[n]}))), \mathrm{NR}^*(\boldsymbol{a}, x) = g^{\prod_{i=1}^{n} \boldsymbol{a}[i]^{x[i]}},$$

where $\boldsymbol{a} = (\boldsymbol{a}[1], \cdots, \boldsymbol{a}[n]) \in (Z_q^*)^{n+1}$ is the key for the PRF, $x = (x[1], \cdots, x[n] \in \{0,1\}^n)$ is the input of the PRF, n is the parameter of security level, $G = \langle g \rangle$ is a group of order q, h is a collision resistant hash function. When $(g^{\boldsymbol{a}[1]}, \cdots, g^{\boldsymbol{a}[n]})$ are precomputed, the computation of F only needs one exponentiation . However, when embedded into our scheme, the key of the PRF $\boldsymbol{a}$ is randomly generated for every ciphertext. That is, we need to compute $(g^{\boldsymbol{a}[1]}, \cdots, g^{\boldsymbol{a}[n]})$ for every computation of the PRF. As a result, the computation of the PRF needs $n+1$ exponentiations.

Moreover, the key space of the RKA secure PRF is a vector that contains n elements. To embed this PRF into our scheme, the KEM part of our scheme needs to encapsulate the key $\boldsymbol{a}$ which contains n elements. This will significantly enlarge the ciphertext.

In this paper, we propose a direct construction of RKA secure authenticated encryption scheme with respect to affine functions that do not contain constant functions. Concretely, let $f(x) = ax + b$ be an affine function, we consider affine functions that $a \neq 0$. Let π be an AE-OT secure authenticated encryption scheme, G a group with order N, $g \in G$ a generator of G, $\mathrm{H} : Z_N \to \{0,1\}^{l_\kappa}$ a 4-wise independent hash function, r a random number chosen from Z_N, our RKA secure authenticated encryption scheme encrypts the plaintext message m as follows:

$$u \leftarrow g^r, \kappa \leftarrow \mathrm{H}(u^k, u), e \leftarrow \pi.\mathrm{E}_\kappa(m),$$

where l_κ is the length of κ, $\pi.\mathrm{E}_\kappa(\cdot)$ denote the encryption algorithm with the key κ, and the ciphertext is (u, e). We prove that if π is AE-OT secure and the DDH (Decisional Diffie-Hellman) assumption holds in G, then our new authenticated encryption scheme is RKA secure.

Technical Relation to Hofheinz's Scheme. To prevent the entropy leakage of the authentication tag added to the ciphertext, Hofheinz's [33] solution is

embedding the plaintext into an encrypted LAF. Concretely, for a given public key Fpk, if t is a lossy tag, then $\mathrm{LAF}_{Fpk,t}([sk]_{Z_p^n})$ only depends on a linear combination of its input $[sk]_{Z_p^n} \in Z_p^n$, here $[sk]_{Z_p^n}$ denotes encoding the private key sk into Z_p^n. In particular, the coefficients of the linear combination only depend on Fpk. That is, for different tags t_i, $\mathrm{LAF}_{Fpk,t_i}([sk]_{Z_p^n})$ only leaks the same linear function of $[sk]_{Z_p^n}$. However, when considering KDM security with respect to richer functions such as affine functions, $\mathrm{LAF}_{Fpk,t_i}([f_i(sk)]_{Z_p^n})$ may leak all the entropy of $[sk]_{Z_p^n}$, here $f_1, \cdots, f_l$ are affine functions chosen by the adversary. Thus, Hofheinz's scheme can only achieve CIRC-CCA (circular security against chosen ciphertext attacks) security.

In our new construction, different from the approach of Hofheinz [33], we divide the entropy of the private key into two independent parts and derive the first part by using an entropy filter to construct an authentication tag. We prove that the entropy in the first part of the private key is enough to prevent the adversary from constructing a valid key-dependent encryption. Compared with the LAF used by Hofheinz, the construction of our entropy filter is simpler and more efficient.

To prevent the entropy leakage of the authentication tag in the challenge ciphertext, Hofheinz's [33] solution is "lossy". The lossy property of LAF guarantees that, information theoretically, little information about the private key is released. To this end, we use a way of "hiding". Concretely, the keys for the authenticated encryption are hidden from the adversary by using linear combinations of the second part of the private key. According to the definition of RKA security, the encryption scheme is secure even when the keys are linearly dependent. Thus, the authentication tags are perfectly hidden from the adversary.

1.2 Outline

In section 2 we review the definitions of public key encryption scheme, KDM-CCA security, decisional composite residuosity assumption, authenticated encryption, decisional Diffie-Hellman assumption and leftover hash lemma. In section 3 we propose the formal definition of RKA secure authenticated encryption scheme and an efficient construction. In section 4 we propose our new KDM-CCA secure scheme and the security proof. Finally we give the conclusion in section 5.

2 Definitions

We write $[n] = \{1, \cdots, n\}$. In describing probabilistic processes, if S is a finite set, we write $s \xleftarrow{R} S$ to denote assignment to s of an element sampled from uniform distribution on S. If A is a probabilistic algorithm and x an input, then $A(x)$ denotes the output distribution of A on input x. Thus, we write $y \leftarrow A(x)$ to denote of running algorithm A on input x and assigning the output to the variable y. For an integer $v \in N$, we let U_v denote the uniform distribution over

$\{0,1\}^v$, the bit-string of length v. The *min-entropy* of a random variable X is defined as

$$\mathrm{H}_\infty(X) = -\lg(\max_{x\in\mathcal{X}} \Pr[X = x]).$$

The statistical distance between two random variables X, Y is defined by

$$\mathrm{SD}(X,Y) = \frac{1}{2}\sum_x |\Pr[X = x] - \Pr[Y = x]|.$$

2.1 Public Key Encryption Scheme

A public key encryption scheme consists of the following algorithms:

- **Setup**(l): A probabilistic polynomial-time setup algorithm takes as input a security parameter l and outputs the system parameter prm. We write $prm \leftarrow \mathrm{Setup}(l)$.
- **Gen**(prm): A probabilistic polynomial-time key generation algorithm takes as input the system parameter prm and outputs a public key pk and a private key sk. We write $(pk, sk) \leftarrow \mathrm{Gen}(prm)$.
- **E**(pk, m): A probabilistic polynomial-time encryption algorithm takes as input a public key pk and a message m, and outputs a ciphertext c. We write $c \leftarrow \mathrm{E}_{pk}(m)$.
- **D**(sk, c): A decryption algorithm takes as input a ciphertext c and a private key sk, and outputs a plaintext m. We write $m \leftarrow \mathrm{D}_{sk}(c)$.

For correctness, we require $\mathrm{D}_{sk}(\mathrm{E}_{pk}(m)) = m$ for all (pk, sk) output by $\mathrm{Gen}(prm)$ and all $m \in M$ (M denotes the message space).

2.2 KDM-CCA Security

A public key encryption scheme is n-KDM-CCA secure w.r.t F if the advantage of any adversary in the following game is negligible in the security parameter l:

- **Step 1:** The challenger runs $\mathrm{Setup}(l)$ to generate the system parameter prm, then runs $\mathrm{Gen}(prm)$ to obtain n keypairs $(pk_i, sk_i), i = 1, \cdots, n$. It sends prm and $(pk_1, \cdots, pk_n)$ to the adversary.
- **Step 2:** The adversary issues decryption queries with (c_j, i), where $1 \le j \le Q_d, 1 \le i \le n$, Q_d denotes the total number of decryption queries. With each query, the challenger sends $m_j \leftarrow \mathrm{D}_{sk_i}(c_j)$ to the adversary.
- **Step 3:** The adversary issues encryption queries with (f_λ, i), where $f_\lambda \in F, 1 \le \lambda \le Q_e, 1 \le i \le n$, Q_e denotes the total number of encryption queries. With each query, the challenger sends $c^*_\lambda \leftarrow \mathrm{E}_{pk_i}(m_{\lambda b})$ to the adversary, where $m_{\lambda 0} = \{0\}^{l_\lambda}, m_{\lambda 1} = f_\lambda(sk_1, \cdots, sk_n)$, $l_\lambda = |m_{\lambda 1}|$, $b \in \{0,1\}$ is a random bit selected by the challenger (note that the challenger chooses b only once).

– **Step 4:** The adversary issues decryption queries just as in step 2, the only restriction is that the adversary can not ask the decryption of c_λ^* for $1 \leq \lambda \leq Q_e$.
– **Step 5:** Finally, the adversary outputs b' as the guess of b.

The adversary's advantage is defined as:

$$\mathrm{AdvKDM}_{\mathcal{A},n}^{\mathrm{cca}} = |\Pr[b' = b] - 1/2|.$$

As a special case of n-KDM-CCA, if $F = \{f_\lambda : f_\lambda(sk_1, \cdots, sk_n) = sk_\lambda, \lambda \in [n]$ we say that the public key encryption scheme is n-CIRC-CCA secure.

2.3 Decisional Composite Residuosity Assumption

Let $N = pq$, p and q are safe primes, the quadratic residuosity group over $Z_{N^s}^*$ is defined as $\mathrm{QR}_{N^s} = \{u^2 \mod N^s | u \in Z_{N^s}^*\}$, the square composite residuosity group as $\mathrm{SCR}_{N^s} = \{v^{N^{s-1}} \mod N^s | v \in \mathrm{QR}_{N^s}\}$, the root of the unity group as $\mathrm{RU}_{N^s} = \{T^r \mod N^s | r \in [N^{s-1}], T = 1 + N \mod N^s\}$, consider the experiment $\mathrm{Exp}_{\mathcal{A}}^{\mathrm{dcr}}$:

$$W_0 \xleftarrow{R} \mathrm{QR}_{N^s}, W_1 \xleftarrow{R} \mathrm{SCR}_{N^s}, b \xleftarrow{R} \{0,1\},$$

$$b' \leftarrow \mathcal{A}(N, W_b), \text{return } b'.$$

Denote $\Pr[Suc_{\mathcal{A}}^{dcr}] = \Pr[b' = b]$ as the probability that $\mathcal{A}$ succeeds in guessing b. We define the advantage of $\mathcal{A}$ in $\mathrm{Exp}_{\mathcal{A}}^{\mathrm{dcr}}$ as

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{dcr}} = |\Pr[b' = b] - \frac{1}{2}|.$$

We say that the decisional composite residuosity (DCR) assumption holds if $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{dcr}}$ is negligible for all polynomial-time adversaries $\mathcal{A}$.

We review a lemma of [20] which is useful to the security proof of our scheme. Let $\mathcal{A}$ be an adversary and $s \geq 2$ be an integer, define game IV2 as follows.

$$\text{IV2: } g_1, g_2 \xleftarrow{R} \mathrm{SCR}_{N^s}, b' \leftarrow \mathcal{A}^{\mathcal{O}_{iv2}(\delta,\bar{\delta})}(N, g_1, g_2).$$

In the game above $\mathcal{A}$ is allowed to make polynomial number queries. In each query, $\mathcal{A}$ can send $(\delta, \bar{\delta} \in Z_{N^{s-1}})$ to the oracle $\mathcal{O}_{iv2}$. $\mathcal{O}_{iv2}(\delta, \bar{\delta})$ then selects $r \in [\lfloor N/4 \rfloor]$ randomly and returns $(g_1^r T^\delta, g_2^r T^{\bar{\delta}})$ if $b = 1$ and (g_1^r, g_2^r) otherwise, where $b \in \{0,1\}$ is randomly selected. The advantage of $\mathcal{A}$ is defined to be

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{iv2}} = |\Pr[b' = b] - \frac{1}{2}|.$$

Lemma 1. *No polynomial-time adversary can have non-negligible advantage in IV2 under the DCR assumption.*

Our definition of IV2 follows from the version in [40], which is slightly different from the original definition in [20].

Note that the discrete logarithm $\mathrm{dlog}_T(X) := x$ for $X \in \mathrm{RU}_{N^s}$ and $x \in N^{s-1}$ can be efficiently computed [26, 42].

2.4 Authenticated Encryption

We review the security definitions of the authenticated encryption scheme. An authenticated encryption (AE) scheme consists of three algorithms:

- AE.Setup(l): The setup algorithm takes as input the security parameter l, and outputs public parameters $param$ and the key k of the AE scheme. We write $(param, k) \leftarrow \text{AE.Setup}(l)$.
- $\text{AE.E}_k(m)$: The encryption algorithm takes as inputs a key k and a message m and outputs a ciphertext χ. We write $\chi \leftarrow \text{AE.E}_k(m)$
- $\text{AE.D}_k(\chi)$: The decryption algorithm takes as inputs a key k, a ciphertext χ and outputs a message m or the rejection symbol $\perp$. We write $m \leftarrow \text{AE.D}_k(\chi)$.

We require that for all $k \in \{0,1\}^{l_k}$ (l_k denotes the length of k), $m \in \{0,1\}^*$, we have:

$$\text{AE.D}_k(\text{AE.E}_k(m)) = m.$$

An AE scheme is IND-OT (indistinguishability against one-time attacks) secure if the advantage of any PPT (Probabilistic Polynomial Time) adversary $\mathcal{A}$ in the following game is negligible in the security parameter l:

1. The challenger randomly generates an appropriately sized key k.
2. The adversary $\mathcal{A}$ queries the encryption oracle with two messages m_0 and m_1 such that $|m_0| = |m_1|$. The challenger computes

$$b \overset{R}{\leftarrow} \{0,1\}, \chi^* \leftarrow \text{AE.E}_k(m_b)$$

   and responds with χ^*.
3. Finally, $\mathcal{A}$ outputs a guess b' .

The advantage of $\mathcal{A}$ is defined as $\text{Adv}_{\mathcal{A}}^{\text{ind-ot}}(l) = |\Pr[b = b'] - 1/2|$. We say that the AE is one-time secure in the sense of indistinguishability if $\text{Adv}_{\mathcal{A}}^{\text{ind-ot}}(l)$ is negligible.

An AE scheme is INT-OT (one-time secure in the sense of ciphertext integrity) secure if the advantage of any PPT adversary $\mathcal{A}$ in the following game is negligible in the security parameter l:

1. The challenger randomly generates an appropriately sized key k.
2. The adversary $\mathcal{A}$ queries the encryption oracle with a message m. The challenger computes

$$\chi^* \leftarrow \text{AE.E}_k(m)$$

   and responds with χ^*.
3. Finally, the adversary $\mathcal{A}$ outputs a ciphertext $\chi \neq \chi^*$ such that $\text{AE.D}_k(\chi) \neq \perp$.

The advantage of $\mathcal{A}$ is defined as

$$\text{Adv}_{\mathcal{A}}^{\text{int-ot}}(l) = \Pr[\text{AE.D}_k(\chi) \neq \perp].$$

We say that the AE is one-time secure in the sense of ciphertext integrity if $\text{Adv}_{\mathcal{A}}^{\text{int-ot}}(l)$ is negligible. An AE is one-time secure (AE-OT) iff it is IND-OT secure and INT-OT secure.

2.5 Decisional Diffie-Hellman Assumption

Let G be a group of large prime order q, g is a generator of G, consider the experiment $\mathrm{Exp}^{\mathrm{ddh}}_{\mathrm{G},\mathcal{A}}$:

$$(x, y, z) \xleftarrow{R} Z_q^*; W_0 \leftarrow g^z; W_1 \leftarrow g^{xy}; b \xleftarrow{R} \{0,1\}$$

$$b' \leftarrow \mathcal{A}(g, g^x, g^y, W_b).$$

We define the advantage of $\mathcal{A}$ as

$$\mathrm{Adv}^{\mathrm{ddh}}_{\mathcal{A}} = |\Pr[b' = b] - 1/2|.$$

We say that the DDH assumption holds if $\mathrm{Adv}^{\mathrm{ddh}}_{\mathcal{A}}$ is negligible for all polynomial-time adversaries $\mathcal{A}$.

2.6 Leftover Hash Lemma

Multiple versions of LHL (Leftover Hash Lemma) have been proposed, we recall the generalized version in [37]: if H is 4-wise independent, then $(\mathrm{H}, \mathrm{H}(X), \mathrm{H}(\tilde{X}))$ is close to uniformly random distribution.

Lemma 2. (**Generalized Leftover Hash Lemma**) *Let $\mathcal{H} = \{H : \mathcal{X} \to \{0,1\}^v\}$ be a family of 4-wise independent hash functions, $(X, \tilde{X}) \in \mathcal{X} \times \mathcal{X}$ be two random variables where $H_\infty(X) \geq \kappa$, $H_\infty(\tilde{X}) \geq \kappa$ and $\Pr[X = \tilde{X}] \leq \delta$. Then for $H \xleftarrow{R} \mathcal{H}$ and $U_{2l} \xleftarrow{R} \{0,1\}^{2l}$,*

$$SD((H, H(X), H(\tilde{X})), (H, U_{2l})) \leq \sqrt{1+\delta} \cdot 2^{l-\kappa/2} + \delta.$$

3 RKA Secure Authenticated Encryption

3.1 Definition of RKA Security for Authenticated Encryption

Following [12], we give a formal definition for the RKA security of AE schemes. Similar as the definition of AE-OT security, the definition of RKA security includes two aspects: indistinguishability security against related key attacks (IND-RKA) and integrity security against related key attacks (INT-RKA).

Definition 1. *An AE scheme is IND-RKA secure with respect to a class of related-key deriving functions F if the advantage of any PPT adversary $\mathcal{A}$ in the following game is negligible in the security parameter l.*

1. The challenger randomly generates an appropriately sized key k for the security parameter l.

2. The adversary $\mathcal{A}$ makes a sequence of related-key encryption queries with m_{i0}, m_{i1}, f_i such that $|m_{i0}| = |m_{i1}|$. Here $1 \leq i \leq Q$, Q denotes the number of related-key encryption queries made by the adversary $\mathcal{A}$, m_{i0} and m_{i1} are two messages, $f_i \in F$, F is a class of related-key deriving functions. The challenger chooses $b \in \{0,1\}$ randomly and responds with a challenge ciphertext for each query of $\mathcal{A}$ computed as follows:

$$\chi_i^* \leftarrow \mathrm{AE.E}_{f_i(k)}(m_{ib}).$$

3. Finally, $\mathcal{A}$ outputs a guess b' .

The advantage of $\mathcal{A}$ is defined as $\mathrm{Adv}_{\mathcal{A}}^{\text{ind-rka}}(l) = |\Pr[b = b'] - 1/2|$.

Definition 2. *An AE scheme is INT-RKA secure with respect to a class of related-key deriving functions F, if the advantage of any PPT adversary $\mathcal{A}$ in the following game is negligible in the security parameter l.*

1. The challenger randomly generates an appropriately sized key k for the security parameter l.
2. The adversary $\mathcal{A}$ makes a sequence of related-key encryption queries with m_i, f_i. Here $1 \leq i \leq Q$, Q denotes the number of related-key encryption queries made by the adversary $\mathcal{A}$, m_i is a plaintext message, $f_i \in F$, F is a class of related-key deriving functions. The challenger responds with a challenge ciphertext for each query of $\mathcal{A}$ computed as follows:

$$\chi_i^* \leftarrow \mathrm{AE.E}_{f_i(k)}(m_i).$$

3. Finally, the adversary $\mathcal{A}$ outputs a ciphertext χ and a related-key deriving function f such that $(f, \chi) \neq (f_i, \chi_i^*)$ and $\mathrm{AE.D}_{f(k)}(\chi) \neq \perp$.

The advantage of $\mathcal{A}$ is defined as

$$\mathrm{Adv}_{\mathcal{A}}^{\text{int-rka}}(l) = \Pr[\mathrm{AE.D}_k(\chi) \neq \perp].$$

Finally, the RKA security of the AE scheme is defined as follows:

Definition 3. *An AE is RKA secure iff it is IND-RKA secure and INT-RKA secure.*

3.2 Construction of RKA Secure Authenticated Encryption

We propose a randomized RKA secure authenticated encryption scheme with respect to affine functions that do not contain constant functions. Concretely, let $f(x) = ax + b$ be an affine function, we consider affine functions that $a \neq 0$.

Let π be an AE-OT secure authenticated encryption scheme, our new construction $\bar{\pi}$ is described as follows:

– **Setup**(l): Randomly choose two safe primes p and q that $2pq+1$ is also a prime, then compute:

$$N \leftarrow pq, \bar{N} \leftarrow 2N+1, g \xleftarrow{R} \mathrm{QR}_{\bar{N}}, param \leftarrow (N, \bar{N}, g), k \xleftarrow{R} Z_N.$$

– **Encryption:** The encryption algorithm takes as inputs a key $k \in Z_N$ and a message m and computes as follows:

$$r \xleftarrow{R} Z_N, u \leftarrow g^r, \kappa \leftarrow \mathrm{H}(u^k, u),$$

$$e \leftarrow \pi.\mathrm{E}_\kappa(m), \chi \leftarrow (u, e).$$

Here $\mathrm{H} : QR_{\bar{N}} \times QR_{\bar{N}} \rightarrow \{0,1\}^{l_\kappa}$ is a 4-wise independent universal hash function, l_κ is the length of κ.

– **Decryption**: The decryption algorithm takes as inputs a key k, a ciphertext $\chi = (u, e)$ and computes as follows:

$$\kappa \leftarrow \mathrm{H}(u^k, u), m \leftarrow \pi.\mathrm{D}_\kappa(e).$$

We prove that if π is AE-OT secure and the DDH assumption holds in $\mathrm{QR}_{\bar{N}}$, then our new authenticated encryption scheme is RKA secure.

Theorem 1. *Assume the DDH assumption holds in $QR_{\bar{N}}$, π is AE-OT secure, then $\bar{\pi}$ is RKA secure with respect to affine functions $f(x) = ax + b$ that $a \neq 0$.*

According to the definition of the RKA security of AE scheme, we need to prove two lemmas as follows.

Lemma 3. *Assume the DDH assumption holds in $QR_{\bar{N}}$, π is AE-OT secure, then $\bar{\pi}$ is IND-RKA secure with respect to affine functions $f(x) = ax + b$ that $a \neq 0$.*

Lemma 4. *Assume the DDH assumption holds in $QR_{\bar{N}}$, π is AE-OT secure, then $\bar{\pi}$ is INT-RKA secure with respect to affine functions $f(x) = ax + b$ that $a \neq 0$.*

Proof of Lemma 3: The proof is via a sequence of games involving the challenger $\mathcal{C}$ and the adversary $\mathcal{A}$. Let W_i be the event that $\mathcal{A}$ guesses b correctly in Game i.

– **Game 0:** This game is the actual IND-RKA game. Hence,we have:

$$\Pr[W_0] = 1/2 + \mathrm{Adv}^{\text{ind-rka}}_{\mathcal{A}}. \tag{1}$$

– **Game 1:** This game is exactly like Game 0, except that the challenge cipertexts are computed using g^k instead of k. That is, let $\hat{g} = g^k$, the keys for π are computed as $\kappa_i \leftarrow \mathrm{H}(\hat{g}^{r_i a_i} g^{r_i b_i}, g^{r_i})$. It is clear that Game 0 and Game 1 are identical from the point view of the adversary $\mathcal{A}$, hence we have:

$$\Pr[W_0] = \Pr[W_1]. \tag{2}$$

- **Game** 1.i**:** Denote Game 1.0 as Game 1, for $1 \leq i \leq Q$, Game 1.i is exactly like Game 1.$(i-1)$ except that the key for π in the ith ciphertext is computed as $\kappa_i \leftarrow \mathrm{H}(\hat{g}^{r_i^* a_i} g^{r_i b_i}, g^{r_i})$, where $r_i^* \neq r_i$ is randomly chosen from Z_N. It is clear that if the adversary $\mathcal{A}$ can distinguish Game 1.i from Game 1.$(i-1)$, then we can break the DDH assumption. Briefly, given a DDH challenge $(g, \hat{g}, g^r, \hat{g}^{r^*})$, to compute the ith ciphertext, the challenger sets $u_i = g^r, \kappa_i = H(\hat{g}^{r^* a_i} g^{r b_i}, u_i)$. The computation of the other ciphertexts is the same as in Game 1.$(i-1)$. It is clear that when $r = r^*$, it is just the case in Game 1.(i-1), when $r \neq r^*$ it is just the case in Game 1.i. Thus, if the adversary $\mathcal{A}$ can distinguish Game 1.i from Game 1.$(i-1)$, then the challenger can break the DDH assumption. Hence we have:

$$\Pr[W_{1.i-1}] \leq \Pr[W_{1.i}] + \mathrm{Adv}_{\mathcal{A}}^{\mathrm{ddh}}. \tag{3}$$

– **Game 2:** This game is exactly Game 1.Q. It is clear that, when $a_i \neq 0$ the keys for the challenge ciphertexts $\kappa_i = \mathrm{H}(\hat{g}^{r_i^* a_i} g^{r_i b_i}, g^{r_i})$ are randomly distributed. According to the IND-OT security of π, we have:

$$\Pr[W_2] \leq 1/2 + Q\mathrm{Adv}_{\mathcal{A}}^{\text{ind-ot}}. \tag{4}$$

From equations $(1) - (4)$ we have:

$$\mathrm{Adv}_{\mathcal{A}}^{\text{ind-rka}} \leq Q\mathrm{Adv}_{\mathcal{A}}^{\mathrm{ddh}} + Q\mathrm{Adv}_{\mathcal{A}}^{\text{ind-ot}}.$$

This completes the proof of lemma 3. □

Proof of Lemma 4: The proof is via a sequence of games involving the challenger $\mathcal{C}$ and the adversary $\mathcal{A}$. Let W_i be the event that $\mathcal{A}$ outputs a valid ciphertext in Game i.

– **Game 0:** This game is the actual INT-RKA game. When responding to a related-key encryption query with m_i, f_i, where $f_i(k) = a_i k + b_i$, $\mathcal{C}$ computes as follows:

$$r_i \overset{R}{\leftarrow} Z_N, u_i \leftarrow g^{r_i}, \kappa_i \leftarrow \mathrm{H}(u_i^{a_i k + b_i}, u_i),$$
$$e_i \leftarrow \pi.\mathrm{E}_{\kappa_i}(m_i), \chi_i \leftarrow (u_i, e_i).$$

– **Game 1:** This game is exactly like Game 0, except that the challenge ciphertexts are computed using g^k instead of k. That is, let $\hat{g} = g^k$, the keys for π are computed as $\kappa_i \leftarrow \mathrm{H}(\hat{g}^{r_i a_i} g^{r_i b_i}, g^{r_i})$. It is clear that Game 0 and Game 1 are identical from the point view of the adversary $\mathcal{A}$, hence we have:

$$\Pr[W_0] = \Pr[W_1]. \tag{5}$$

- **Game** 1.i**:** Denote Game 1.0 as Game 1, for $1 \leq i \leq Q$, Game 1.i is exactly like Game 1.$(i-1)$ except that the key for π in the ith ciphertext is computed as $\kappa_i \leftarrow \mathrm{H}(\hat{g}^{r_i^* a_i} g^{r_i b_i}, g^{r_i})$, where $r_i^* \neq r_i$ is randomly chosen from Z_N. It is clear that if the adversary $\mathcal{A}$ can distinguish Game 1.i from Game 1.$(i-1)$, then we can break the DDH assumption. Hence we have:

$$\Pr[W_{1.i-1}] \leq \Pr[W_{1.i}] + \mathrm{Adv}_{\mathcal{A}}^{\mathrm{ddh}}. \tag{6}$$

– **Game 2:** This game is exactly Game 1.Q. Denote $\chi = (u = g^r, e = \pi.\mathrm{E}_\kappa(m)), f(k) = ak + b$ as the forged ciphertext and the related-key deriving function, we consider three cases as follows:
  - Case 1: $f = f_i, u = u_i, e \neq e_i$. In this case we have $\kappa = \kappa_i$, if χ is a valid ciphertext then we get a forged ciphertext of e_i. It is clear that the keys for the challenge ciphertexts $\kappa_i = \mathrm{H}(\hat{g}^{r_i^* a_i} g^{r_i b_i}, g^{r_i})$ are randomly distributed. According to the INT-OT security of π, we have:
$$\Pr[W_2|Case1] \leq Q\mathrm{Adv}_{\mathcal{A}}^{\text{int-ot}}. \tag{7}$$
  - Case 2: $f \neq f_i, u = u_i$. In this case, we consider two subcases as follows:
    * Case 2.1: $r_i^* ak + r_i b = r_i^* a_i k + r_i b_i$. It is clear that, if the adversary $\mathcal{A}$ submits such related-key deriving function, we can break the discrete logarithm assumption. Concretely, given $g, \hat{g} = g^k$, the simulator $\mathcal{S}$ can play Game 2 with $\mathcal{A}$. When $\mathcal{A}$ submits χ, f, $\mathcal{S}$ computes $k_i = \frac{r_i(b_i - b)}{r_i^*(a - a_i)}$ and test whether $\hat{g} = g^{k_i}$. Let ϵ_{dlg} be the probability that any adversary breaks the discrete logarithm assumption, we have:
$$\Pr[Case2.1] \leq \epsilon_{dlg}. \tag{8}$$
    * Case 2.2: $r_i^* ak + r_i b \neq r_i^* a_i k + r_i b_i$. In this subcase, $\hat{g}^{r_i^* a} g^{r_i b} \neq \hat{g}^{r_i^* a_i} g^{r_i b_i}$. Since r_i^* is randomly selected from Z_N and $a \neq 0, a_i \neq 0$, we have:
$$\mathrm{H}_\infty(\hat{g}^{r_i^* a} g^{r_i b}) = \mathrm{H}_\infty(\hat{g}^{r_i^* a_i} g^{r_i b_i}) = l_N,$$
    where l_N is the length of N. According to the property of 4-wise independent hash functions, $\mathrm{H}(\hat{g}^{r_i^* a} g^{r_i b}, u), \mathrm{H}(\hat{g}^{r_i^* a_i} g^{r_i b_i}, u_i)$ is randomly distributed from the point view of the adversary $\mathcal{A}$. Hence, we have:
$$\Pr[W_2|Case2.2] \leq \mathrm{Adv}_{\mathcal{A}}^{\text{int-ot}}. \tag{9}$$
  - Case 3: $u \neq u_i$. Since the information of k is statistically hidden by r_i^*, we have:
$$\mathrm{H}_\infty(u^{ak+b}) = \mathrm{H}_\infty(u_i^{a_i k + b_i}) = l_N,$$
    where l_N is the length of N. According to the property of 4-wise independent hash functions, $\mathrm{H}(u^{ak+b}, u), \mathrm{H}(u_i^{a_i k + b_i}, u_i)$ is randomly distributed from the point view of the adversary $\mathcal{A}$. Hence, we have:
$$\Pr[W_2|Case3] \leq \mathrm{Adv}_{\mathcal{A}}^{\text{int-ot}}. \tag{10}$$

From equations $(7) - (10)$ we have:

$$\Pr[W_2] \leq Q\mathrm{Adv}_{\mathcal{A}}^{\text{int-ot}} + \epsilon_{dlg}. \tag{11}$$

From the equations $(5), (6), (11)$ we have that:

$$\begin{aligned} \mathrm{Adv}_{\mathcal{A}}^{\text{int-rka}} &= \Pr[W_0] \\ &\leq Q\mathrm{Adv}_{\mathcal{A}}^{\text{ddh}} + Q\mathrm{Adv}_{\mathcal{A}}^{\text{int-ot}} + \epsilon_{dlg}. \end{aligned} \tag{12}$$

This completes the proof of lemma 4. □

4 KDM-CCA Secure Scheme

4.1 The Idea of Our Construction

Before formal description, we give some intuition of our construction. Just as we mentioned in section 1.1, existing KDM-CPA schemes [19, 4, 20, 40] are very suitable to be used as a key-dependent message encoding. To encode the messages depending on the private key of the KEM part, the encoding scheme must share the same parameters (especially the private key) with the KEM part. For this reason, we first choose a KDM-CPA scheme, then translate it into a KEM scheme. Concretely, we choose the KDM-CPA scheme in [40] as the key-dependent message encoding scheme and translate it into a KEM by replacing the plaintext with a randomly selected key k. Briefly the ciphertext of the hybrid encryption can be described as:

$$u = g^r, e = h^r T^k, v = \bar{\pi}.\mathrm{E}_k(g^{\tilde{r}}||h^{\tilde{r}}T^m),$$

where $g \in \mathrm{SCR}_{N^s}, s \geq 2, x \in [\lfloor N^2/4 \rfloor], h = g^x, r, \tilde{r} \in [\lfloor N/4 \rfloor]$, $\bar{\pi}$ is an RKA secure authenticated encryption scheme. Given the public key (g, h), we have $h = g^{x \mod \phi(N)/4} \mod N^s$. That is, conditioned on the public key, $x \mod N$ is hidden from the adversary information theoretically. Thus, the entropy of the private key is $x \mod N$.

To divide the entropy of the private key into two parts independent of each other, we enlarge the entropy by extending the public key and the private key. As a result, the ciphertext of the hybrid encryption is extended as:

$$u_1 = g_1^r, u_2 = g_2^r, e = h^r T^k, v = \bar{\pi}.\mathrm{E}_k(g_1^{\tilde{r}}||g_2^{\tilde{r}}||h^{\tilde{r}}T^m),$$

where $g_1, g_2 \in \mathrm{SCR}_{N^s}, x_1, x_2 \in [\lfloor N^2/4 \rfloor], h = g_1^{x_1} g_2^{x_2}$. It is clear that, conditioned on the public key, the adversary can only get

$$h = g_1^{x_1 \mod \phi(N)/4} g_2^{x_2 \mod \phi(N)/4} \mod N^s.$$

The entropy of the private key can be divided into two parts: the first part is the entropy contained in $(x_1 \mod \phi(N)/4, x_2 \mod \phi(N)/4)$, the second part is the entropy contained in $(x_1 \mod N, x_2 \mod N)$. It is easy to construct an entropy filter to derive the first part of the entropy from the key-dependent messages as $\theta(f(x_1, x_2)) = g_1^{f(x_1,x_2)}$. To prevent the adversary from getting a valid key-dependent encryption by modifying the challenge ciphertexts, we use the universal hash function H to construct the authentication tag as $t = \mathrm{H}(u_1||u_2||e||\theta(f(x_1, x_2)))$.

In order to protect the key of the RKA secure authenticated encryption scheme by using the second part of the entropy, we modify the KEM part of the hybrid encryption slightly as:

$$u_1 = g_1^r \mod N^2, u_2 = g_2^r \mod N^2, e = h^r T^k \mod N^2.$$

Since $g_1 \mod N^2, g_2 \mod N^2 \in \mathrm{SCR}_{N^2}$, the KEM part is now computed in the group of SCR_{N^2}. In this case we have $e = h^r T^k \mod N^2 = h^r T^{k \mod N} \mod N^2$. That is, the range of k is now shrunk to $[N]$ from $[N^{s-1}]$. When we use (x_1, x_2) to protect k, only the second part of the entropy will be derived out.

4.2 The Proposed Scheme

– **Setup**(l): Randomly choose two safe primes p and q that $2pq+1$ is also a prime, then compute:

$$N \leftarrow pq, g_1, g_2 \overset{R}{\leftarrow} \mathrm{SCR}_{N^s}, prm \leftarrow (N, g_1, g_2).$$

– **Key Generation**: For prm, the key generation algorithm computes:

$$x_1, x_2 \overset{R}{\leftarrow} [\lfloor N^2/4 \rfloor], h \leftarrow g_1^{-x_1} g_2^{-x_2},$$

$$pk \leftarrow (h), sk \leftarrow (x_1, x_2).$$

– **Encryption**: For $m \in [N^{s-1}]$, the encryption algorithm computes the ciphertext c as follows:

$$r, \tilde{r} \overset{R}{\leftarrow} [\lfloor N/4 \rfloor], k \overset{R}{\leftarrow} Z_N,$$

$$u_1 \leftarrow g_1^r \mod N^2, u_2 \leftarrow g_2^r \mod N^2, e \leftarrow h^r T^k \mod N^2,$$

$$\tilde{u}_1 \leftarrow g_1^{\tilde{r}} \mod N^s, \tilde{u}_2 \leftarrow g_2^{\tilde{r}} \mod N^s, \tilde{e} \leftarrow h^{\tilde{r}} T^m \mod N^s,$$

$$t \leftarrow \mathrm{H}(u_1||u_2||e||(g_1^m \mod N)), v \leftarrow \bar{\pi}.\mathrm{E}_k(t||\tilde{u}_1||\tilde{u}_2||\tilde{e}), c \leftarrow (u_1, u_2, e, v).$$

where $\mathrm{H} : \{0,1\}^* \rightarrow \{0,1\}^{l_t}$ is a universal hash function.

– **Decryption**: If $eu_1^{x_1}u_2^{x_2} \notin RU_{N^2}$ return the rejection symbol $\perp$, else compute:

$$k \leftarrow \mathrm{dlog}_T(eu_1^{x_1}u_2^{x_2}),$$

$$t||\tilde{u}_1||\tilde{u}_2||\tilde{e} \leftarrow \bar{\pi}.\mathrm{D}_k(v),$$

$$\text{If } \tilde{e}\tilde{u}_1^{x_1}\tilde{u}_2^{x_2} \notin RU_{N^s} \text{ return } \perp,$$

$$m \leftarrow \mathrm{dlog}_T(\tilde{e}\tilde{u}_1^{x_1}\tilde{u}_2^{x_2}),$$

$$\text{If } t = \mathrm{H}(u_1||u_2||e||(g_1^m \mod N)) \text{ return } m, \text{else return } \perp .$$

It is clear that compared with Hofheinz's CIRC-CCA scheme [33], our new scheme is simpler and more efficient. Concretely, the ciphertext of the Hofheinz's scheme contains 6 Z_{N^3}-elements, 43 Z_p-elements ($p \approx N/4$), a chameleon hash randomness, a one-time signature and the verification key, and a symmetric ciphertext (whose size is about one N_{N^2}-element plus some encryption randomness). However, to achieve CIRC-CCA security, we can set $s = 3$ for our scheme, in this case the ciphertext of our new scheme only contains 3 Z_{N^2}-elements, 3 Z_{N^3}-elements, 1 $Z_{\bar{N}}$-elements ($\bar{N} = 2N+1$), a hash value (whose size is about the security parameter l) and the ciphertext expansion of the authenticated encryption scheme (whose size is about twice of the security parameter l).

4.3 Security Proof

Before formal proof, we give an intuition of the 1-KDM-CCA security of our scheme. The n-KDM-CCA security can be achieved by re-randomizing keys and ciphertexts of a single instance of the scheme like in [19, 20]. Our main idea is to achieve KDM-CCA security based on the entropy of the private key. Concretely, let $x_1^{hide} = x_1 \mod N, x_1^{real} = x_1 \mod \phi(N)/4$, $x_2^{hide} = x_2 \mod N, x_2^{real} = x_2 \mod \phi(N)/4$, we have that $h = g_1^{-x_1} g_2^{-x_2} = g_1^{-x_1^{real}} g_2^{-x_2^{real}}$. Hence, x_1^{hide} and x_2^{hide} are information theoretically hidden from the adversary, conditioned on the public key.

In the security reduction, to encrypt $f(x_1, x_2) = a_1x_1 + a_2x_2 + b$, the ciphertext is constructed as $\bar{\pi}.\mathrm{E}_k(t||g_1^{\tilde{r}}T^{a_1}||g_2^{\tilde{r}}T^{a_2}||h^{\tilde{r}}T^b)$. In fact, this ciphertext can be constructed without knowing x_1^{hide} and x_2^{hide}. Thus it will not leak any information of x_1^{hide} and x_2^{hide}.

Let $\log_{g_1} g_2 = w$, we have that, conditioned on the public key, the only information that the adversary gets about x_1^{real} and x_2^{real} is the following equation:

$$\log_{g_1} h = -(x_1^{real} + wx_2^{real}) \mod \phi(N)/4.$$

It is clear that there is entropy in the pair (x_1^{real}, x_2^{real}), since the adversary only gets one equation for two variables. We divide the entropy of the private key into two parts: the first part is the entropy contained in (x_1^{real}, x_2^{real}), the second part is the entropy contained in (x_1^{hide}, x_2^{hide}).

The first part of the entropy is embedded into an authentication tag to prevent the adversary from constructing a valid encryption of an affine function of the private key $f(x_1, x_2) = a_1x_1 + a_2x_2 + b$. Concretely, we embed $g_1^{f(x_1,x_2)} \mod N = g_1^{a_1x_1^{real} + a_2x_2^{real} + b} \mod N$ into an authentication tag t. Note that if $a_2/a_1 = w \mod \phi(N)/4$, then $a_1x_1^{real} + a_2x_2^{real}$ is linearly dependent with $(x_1^{real} + wx_2^{real})$, and $f(x_1, x_2)$ is not randomly distributed. Fortunately, we prove that this case implies the breaking of the discrete logarithm assumption. If $a_2/a_1 \neq w \mod \phi(N)/4$, then $a_1x_1^{real} + a_2x_2^{real}$ is linearly independent with $(x_1^{real} + wx_2^{real})$, and $a_1x_1^{real} + a_2x_2^{real}$ is randomly distributed. In order to place a valid key-dependent decryption query, the adversary would have to guess the value of $a_1x_1^{real} + a_2x_2^{real}$.

The second part of the entropy is used to protect an original key k^*, which is used to derive keys for the authenticated encryption by using affine functions $f(k^*) = rk^* + s$. We show that the decryption oracle will not leak any information of (x_1^{hide}, x_2^{hide}). Thus k^* is perfectly hidden from the adversary. According to the RKA security of the authenticated encryption, the plaintext messages are perfectly protected by the authenticated encryption.

Theorem 2. *Assume the DCR assumption holds in Z_{N^s}, $\bar{\pi}$ is an RKA secure authenticated encryption scheme with respect to affine functions $f(k) = ak + b$ that $a \neq 0$. Then the scheme above is n-KDM-CCA secure with respect to affine functions with the range of $[N^{s-1}]$ for $s \geq 2$.*

The proof is via a sequence of games involving the challenger $\mathcal{C}$ and the adversary $\mathcal{A}$. Let W_δ be the event that $\mathcal{A}$ guesses b correctly in Game δ.

– **Game 0:** This game is the actual n-KDM-CCA game. The challenger $\mathcal{C}$ runs the setup and key generation algorithm, sends the parameters $prm = (g_1, g_2, N)$ and public keys $pk_i = (h_i = g_1^{x_{i1}} g_2^{x_{i2}}), i = 1, \cdots, n$ to the adversary $\mathcal{A}$. When responding to a key-dependent encryption query with (f_λ, i), that $f_\lambda(sk_1, \cdots, sk_n) = \sum_{j=1}^{n}(a_{j\lambda 1}x_{j1} + a_{j\lambda 2}x_{j2}) + b_\lambda \in [N^{s-1}]$, the challenger $\mathcal{C}$ randomly chooses $b \in \{0, 1\}$ and computes as follows:

$$r_\lambda^*, \tilde{r}_\lambda^* \xleftarrow{R} [\lfloor N/4 \rfloor], k_\lambda^* \xleftarrow{R} Z_N,$$

$$m_{\lambda 0} \leftarrow 0, m_{\lambda 1} \leftarrow \sum_{j=1}^{n}(a_{j\lambda 1}x_{j1} + a_{j\lambda 2}x_{j2}) + b_\lambda,$$

$$u_{\lambda 1}^* \leftarrow g_1^{r_\lambda^*} \mod N^2, u_{\lambda 2}^* \leftarrow g_2^{r_\lambda^*} \mod N^2, e_\lambda^* \leftarrow h_i^{r_\lambda^*} T^{k_\lambda^*} \mod N^2,$$

$$\tilde{u}_{\lambda 1}^* \leftarrow g_1^{\tilde{r}_\lambda^*} \mod N^s, \tilde{u}_{\lambda 2}^* \leftarrow g_2^{\tilde{r}_\lambda^*} \mod N^s, \tilde{e}_\lambda^* \leftarrow h_i^{\tilde{r}_\lambda^*} T^{m_{\lambda b}} \mod N^s,$$

$$t_\lambda^* \leftarrow \mathrm{H}(u_{\lambda 1}^* || u_{\lambda 2}^* || e_\lambda^* || (g_1^{m_{\lambda b}} \mod N)), v_\lambda^* \leftarrow \bar{\pi}.\mathrm{E}_{k_\lambda^*}(t_\lambda^* || \tilde{u}_{\lambda 1}^* || \tilde{u}_{\lambda 2}^* || \tilde{e}_\lambda^*),$$

$$c_\lambda^* \leftarrow (u_{\lambda 1}^*, u_{\lambda 2}^*, e_\lambda^*, v_\lambda^*).$$

When responding to a decryption query $(c = (u_1, u_2, e, v), i)$ the challenger $\mathcal{C}$ decrypts using the secret key $sk_i = (x_{i1}, x_{i2})$. By definition we have:

$$\mathrm{AdvKDM}_{\mathcal{A},n}^{\mathrm{cca}} = \Pr[W_0] - 1/2. \tag{13}$$

– **Game 1:** This game is exactly like Game 0, except that the key generation algorithm runs as follows:

$$x_1, x_2 \xleftarrow{R} [\lfloor N^2/4 \rfloor], \bar{x}_{i1}, \bar{x}_{i2} \xleftarrow{R} [\lfloor N/4 \rfloor],$$

$$x_{i1} \leftarrow x_1 + \bar{x}_{i1}, x_{i2} \leftarrow x_1 + \bar{x}_{i2}, h_i \leftarrow g_1^{-x_{i1}} g_2^{-x_{i2}},$$

$$pk_i \leftarrow (h_i), sk_i \leftarrow (x_{i1}, x_{i2}),$$

It is clear that in the key generation algorithm above x_{i1}, x_{i2} are chosen from $[\lfloor N^2/4 \rfloor + \lfloor N/4 \rfloor]$ instead of $[\lfloor N^2/4 \rfloor]$. The statistical distance between the uniform distribution over these two domains is about 2^{-l_N}, where l_N is the length of N.
If we use $\phi(N)/4$ instead of $\lfloor N/4 \rfloor$ then, the distributions of the public keys $pk_1, \cdots, pk_n$ are identical in Game 0 and Game 1. Since $\phi(N)/4 = pq, \lfloor N/4 \rfloor = pq + (p+q)/2$, hence the statistical distance between the public keys in Game 0 and Game 1 is bounded by $2^{-l_N/2}$.
As a result, we have:

$$\Pr[W_0] \leq \Pr[W_1] + 2^{-l_N} + 2^{-l_N/2}. \tag{14}$$

– **Game 2:** This game is exactly like Game 1, except that when responding to the key-dependent encryption query, $\tilde{e}^*_\lambda$ and e^*_λ are computed as:

$$e^*_\lambda \leftarrow u^{*-x_{i1}}_{\lambda 1} u^{*-x_{i2}}_{\lambda 2} T^{k^*_\lambda} \mod N^2, \tilde{e}^*_\lambda \leftarrow \tilde{u}^{*-x_{i1}}_{\lambda 1} \tilde{u}^{*-x_{i2}}_{\lambda 2} T^{m_{\lambda b}} \mod N^s.$$

It is clear that $\tilde{u}^{*-x_{i1}}_{\lambda 1} \tilde{u}^{*-x_{i2}}_{\lambda 2} = h_i^{\tilde{r}^*_\lambda}, u^{*-x_{i1}}_{\lambda 1} u^{*-x_{i2}}_{\lambda 2} = h_i^{r^*_\lambda}$. Hence we have:

$$\Pr[W_1] = \Pr[W_2]. \tag{15}$$

– **Game 3:** Game 3 is exactly like Game 2, except that when responding to the key-dependent encryption query, if $b = 1$, then $\tilde{u}^*_{\lambda 1}, \tilde{u}^*_{\lambda 2}, \tilde{e}^*_\lambda$ are computed as follows:

$$\tilde{u}^*_{\lambda 1} \leftarrow g_1^{\tilde{r}^*_\lambda} T^{a_{\lambda 1}} \mod N^s,$$
$$\tilde{u}^*_{\lambda 2} \leftarrow g_2^{\tilde{r}^*_\lambda} T^{a_{\lambda 2}} \mod N^s,$$
$$\tilde{e}^*_\lambda \leftarrow h_i^{\tilde{r}^*_\lambda} T^{b_\lambda + \rho_\lambda} \mod N^s,$$

where $a_{\lambda 1} = \sum_{j=1}^n a_{j\lambda 1}$, $a_{\lambda 2} = \sum_{j=1}^n a_{j\lambda 2}$ and $\rho_\lambda = \sum_{j=1}^n (a_{j\lambda 1}(\bar{x}_{j1} - \bar{x}_{i1}) + a_{j\lambda 2}(\bar{x}_{j2} - \bar{x}_{i2}))$.
It is clear that if the adversary $\mathcal{A}$ can distinguish Game 3 from Game 2, then $\mathcal{C}$ can solve the IV2 problem. Concretely, when receiving g_1, g_2 from the IV2 challenger, $\mathcal{C}$ runs the key generation algorithm to get pk_i, sk_i. When responding to the key-dependent encryption query, if $b = 1$, $\tilde{u}^*_{\lambda 1}, \tilde{u}^*_{\lambda 2}, \tilde{e}^*_\lambda$ are computed as follows:

$$(\tilde{u}^*_{\lambda 1}, \tilde{u}^*_{\lambda 2}) \leftarrow \mathcal{O}_{iv2}(a_{\lambda 1}, a_{\lambda 2}), \tilde{e}^*_\lambda \leftarrow \tilde{u}^{*-x_{i1}}_{\lambda 1} \tilde{u}^{*-x_{i2}}_{\lambda 2} T^{m_{\lambda b}} \mod N^s.$$

Other parts of the ciphertext and the response to the decryption queries are computed as in Game 2. According to the definition of the IV2 problem, $(\tilde{u}^*_{\lambda 1}, \tilde{u}^*_{\lambda 2}) = (g_1^{\tilde{r}^*_\lambda}, g_2^{\tilde{r}^*_\lambda})$ or $(\tilde{u}^*_{\lambda 1}, \tilde{u}^*_{\lambda 2}) = (g_1^{\tilde{r}^*_\lambda} T^{a_{\lambda 1}}, g_2^{\tilde{r}^*_\lambda} T^{a_{\lambda 2}})$. It is easy to verify that in the first case the response to the key-dependent encryption query is identical to that of Game 2. In the second case we have:

$$\begin{aligned}
\tilde{e}^*_\lambda &= \tilde{u}^{*-x_{i1}}_{\lambda 1} \tilde{u}^{*-x_{i2}}_{\lambda 2} T^{m_{\lambda 1}} \\
&= (g_1^{\tilde{r}^*_\lambda} T^{a_{\lambda 1}})^{-x_{i1}} (g_2^{\tilde{r}^*_\lambda} T^{a_{\lambda 2}})^{-x_{i2}} T^{\sum_{j=1}^n (a_{j\lambda 1} x_{j1} + a_{j\lambda 2} x_{j2}) + b_\lambda} \\
&= (g_1^{\tilde{r}^*_\lambda} T^{\sum_{j=1}^n a_{j\lambda 1}})^{-x_{i1}} (g_2^{\tilde{r}^*_\lambda} T^{\sum_{j=1}^n a_{j\lambda 2}})^{-x_{i2}} T^{\sum_{j=1}^n (a_{j\lambda 1} x_{j1} + a_{j\lambda 2} x_{j2}) + b_\lambda} \\
&= h^{\tilde{r}^*_\lambda} T^{\sum_{j=1}^n (a_{j\lambda 1}(x_{j1} - x_{i1}) + a_{j\lambda 2}(x_{j2} - x_{i2})) + b_\lambda} \\
&= h^{\tilde{r}^*_\lambda} T^{\sum_{j=1}^n (a_{j\lambda 1}(\bar{x}_{j1} - \bar{x}_{i1}) + a_{j\lambda 2}(\bar{x}_{j2} - \bar{x}_{i2})) + b_\lambda} \\
&= h^{\tilde{r}^*_\lambda} T^{\rho_\lambda + b_\lambda}
\end{aligned}$$

Hence we have:

$$\Pr[W_2] \leq \Pr[W_3] + \mathrm{Adv}^{\mathrm{iv}2}_{\mathcal{A}}. \tag{16}$$

– **Game 4:** This game is exactly like Game 3, except that when responding to the key-dependent encryption query, the challenger $\mathcal{C}$ randomly chooses $\alpha, \beta \in Z_N, r^* \in [\lfloor N/4 \rfloor]$, computes $u^*_{\lambda 1}, u^*_{\lambda 2}, e^*_\lambda$ as follows:

$$u^*_{\lambda 1} \leftarrow (g_1^{r^*} T^\alpha)^{r^*_\lambda} \mod N^2,$$

$$u^*_{\lambda 2} \leftarrow (g_2^{r^*} T^{\beta})^{r^*_\lambda} \mod N^2,$$
$$e^*_\lambda \leftarrow (u^{*-x_{i1}}_{\lambda 1} u^{*-x_{i2}}_{\lambda 2}) T^{k^*_\lambda} \mod N^2,$$

Similar as in Game 3, if the adversary $\mathcal{A}$ can distinguish Game 4 from Game 3, then $\mathcal{C}$ can solve the IV2 problem. Hence we have:

$$\Pr[W_3] \leq \Pr[W_4] + \mathrm{Adv}^{\mathrm{iv2}}_{\mathcal{A}}. \tag{17}$$

– **Game 5:** This game is exactly like Game 4, except that when responding to the key-dependent encryption query, the challenger $\mathcal{C}$ randomly chooses $k^* \in Z_N$, computes k^*_λ as follows:

$$s^*_\lambda \overset{R}{\leftarrow} Z_N, k^*_\lambda \leftarrow r^*_\lambda k^* + s^*_\lambda \mod N.$$

It is to verify that $k^*_\lambda = r^*_\lambda k^* + s^*_\lambda \mod N$ is uniformly distributed on Z_N. Hence we have:

$$\Pr[W_4] = \Pr[W_5]. \tag{18}$$

– **Game 6:** This game is exactly like Game 5, except that when responding to the decryption query $(c = (u_1, u_2, e, v), i)$, the challenger $\mathcal{C}$ computes k and m by using $\phi(N) = (p-1)(q-1)$ and $sk_i = (x_{i1}, x_{i2})$ as follows:

$$\alpha' \leftarrow \mathrm{dlog}_T(u_1^{\phi(N)})/\phi(N) \mod N, \beta' \leftarrow \mathrm{dlog}_T(u_2^{\phi(N)})/\phi(N) \mod N,$$

$$\gamma' \leftarrow \mathrm{dlog}_T(e^{\phi(N)})/\phi(N) \mod N, k \leftarrow (\alpha' x_{i1} + \beta' x_{i2} + \gamma') \mod N,$$

$$\tilde{\alpha} \leftarrow \mathrm{dlog}_T(\tilde{u}_1^{\phi(N)})/\phi(N) \mod N^{s-1}, \tilde{\beta} \leftarrow \mathrm{dlog}_T(\tilde{u}_2^{\phi(N)})/\phi(N) \mod N^{s-1},$$

$$\tilde{\gamma} \leftarrow \mathrm{dlog}_T(\tilde{e}^{\phi(N)})/\phi(N) \mod N^{s-1}, m \leftarrow (\tilde{\alpha} x_{i1} + \tilde{\beta} x_{i2} + \tilde{\gamma}) \mod N^{s-1}.$$

It is clear that, the computation of the decryption algorithm in Game 6 is identical to that in Game 5, we have:

$$\Pr[W_5] = \Pr[W_6]. \tag{19}$$

– **Game 7:** This game is exactly like Game 6, except that when responding to the decryption query, the challenger returns $\perp$ when $u_1 = u^*_{\lambda 1}, u_2 = u^*_{\lambda 2}, e = e^*_\lambda, v \neq v^*_\lambda$. Since $\bar{\pi}$ is INT-RKA secure and k^* is randomly distributed from the point view of $\mathcal{A}$ (see Game 8 equation 23 for detailed analysis), such ciphertext will be rejected except with the probability of $\mathrm{Adv}^{\text{int-rka}}_{\mathcal{A}}$. Hence we have:

$$\Pr[W_6] \leq \Pr[W_7] + \mathrm{Adv}^{\text{int-rka}}_{\mathcal{A}}. \tag{20}$$

– **Game 8:** This game is exactly like Game 7, except that when responding to the decryption query, the challenger returns $\perp$ when $\tilde{\alpha} \neq 0$ or $\tilde{\beta} \neq 0$ or $\alpha' \neq 0$ or $\beta' \neq 0$.
Let $x_1^{hide} = x_1 \mod N, x_1^{real} = x_1 \mod \phi(N)/4, x_2^{hide} = x_2 \mod N, x_2^{real} = x_2 \mod \phi(N)/4, x_{i1}^{hide} = x_{i1} \mod N, x_{i1}^{real} = x_{i1} \mod \phi(N)/4, x_{i2}^{hide} = x_{i2}$

$\bmod N, x_{i2}^{real} = x_{i2} \mod \phi(N)/4$, $w = \log_{g_1} g_2$, according to the key generation algorithm we have:

$$\begin{aligned} \log_{g_1} h_i &= -(x_{i1}^{real} + w x_{i2}^{real}) \mod \phi(N)/4 \\ &= -(x_1^{real} + \bar{x}_{i1}^{real} + w(x_2^{real} + \bar{x}_{i2}^{real})) \mod \phi(N)/4. \end{aligned} \tag{21}$$

Hence, x_1^{hide} and x_2^{hide} are randomly distributed from the point view of $\mathcal{A}$ conditioned on the public key. According to the encryption oracle k^* is encapsulated in e_λ^* as follows:

$$\begin{aligned} e_\lambda^* &= (u_{\lambda 1}^{*-x_{i1}} u_{\lambda 2}^{*-x_{i2}}) T^{k_\lambda^*} \mod N^2 \\ &= ((g_1^{r^*} T^\alpha)^{r_\lambda^*})^{-x_{i1}} ((g_2^{r^*} T^\beta)^{r_\lambda^*})^{-x_{i2}} T^{(r_\lambda^* k^* + s_\lambda^*)} \mod N^2 \\ &= h_i^{r^* r_\lambda^*} T^{r_\lambda^*(-\alpha x_{i1} - \beta x_{i2} + k^*) + s_\lambda^*} \mod N^2 \\ &= h_i^{r^* r_\lambda^*} T^{r_\lambda^*(-\alpha(x_1 + \bar{x}_{i1}) - \beta(x_2 + \bar{x}_{i2}) + k^*) + s_\lambda^*} \mod N^2 \end{aligned} \tag{22}$$

$$\begin{aligned} k^* &= \frac{\mathrm{dlog}_T(e_\lambda^{*\phi(N)})/\phi(N)}{r_\lambda^*} + \alpha(x_1 + \bar{x}_{i1}) + \beta(x_2 + \bar{x}_{i2}) - \frac{s_\lambda^*}{r_\lambda^*} \mod N \\ &= \frac{\mathrm{dlog}_T(e_\lambda^{*\phi(N)})/\phi(N)}{r_\lambda^*} + \alpha(x_1^{hide} + \bar{x}_{i1}^{hide}) + \beta(x_2^{hide} + \bar{x}_{i2}^{hide}) - \frac{s_\lambda^*}{r_\lambda^*} \mod N \\ &= \frac{\mathrm{dlog}_T(e_\lambda^{*\phi(N)})/\phi(N)}{r_\lambda^*} + \alpha x_1^{hide} + \beta x_2^{hide} + \alpha \bar{x}_{i1}^{hide} + \beta \bar{x}_{i2}^{hide} - \frac{s_\lambda^*}{r_\lambda^*} \mod N. \end{aligned} \tag{23}$$

It is clear that, when $\tilde{\alpha} = 0, \tilde{\beta} = 0, \alpha' = 0, \beta' = 0$, the decryption oracle will not leak any information of the private key. In addition ciphertexts that $u_1 = u_{\lambda 1}^*, u_2 = u_{\lambda 2}^*, e = e_\lambda^*, v \neq v_\lambda^*$ are rejected. Denote Bad as the event that the challenge does not return $\perp$ when $\tilde{\alpha} \neq 0$ or $\tilde{\beta} \neq 0$ or $\alpha' \neq 0$ or $\beta' \neq 0$. We have that if Bad does not happen, the decryption will not leak any information of k^*. Hence k^* is randomly distributed from the point view of $\mathcal{A}$ conditioned on $\neg Bad$. Now we show that, in Game 7 when $\tilde{\alpha} \neq 0$ or $\tilde{\beta} \neq 0$ or $\alpha' \neq 0$ or $\beta' \neq 0$, the challenger will return $\perp$ except with a negligible probability. For clarity, we consider four cases as follows:

- $\tilde{\alpha} \neq 0, \tilde{\beta} \neq 0$: Since k^* is randomly distributed conditioned on $\neg Bad$ and the keys $k_\lambda^* = r_\lambda^* k^* + s_\lambda^*$ are affine functions of k^*, according to the IND-RKA security of $\bar{\pi}$ we have that v_λ^* will not leak any information of x_1^{real} and x_2^{real} except with negligible probability of $\mathrm{Adv}_{\mathcal{A}}^{\text{ind-rka}}$. Hence the only information that the adversary gets about x_1^{real} and x_2^{real} conditioned on the public key and the ciphertexts is equation (21).
  If $\tilde{\beta}/\tilde{\alpha} \neq w \mod \phi(N)/4$, we have that $\log_{g_1} g_1^m = \tilde{\alpha}(x_1^{real} + \bar{x}_{i1}^{real}) + \tilde{\beta}(x_2^{real} + \bar{x}_{i2}^{real}) + \tilde{\gamma} \mod \phi(N)/4$ is linearly independent with equation (21). Thus $t = \mathrm{H}(u_1||u_2||e||g_1^m)$ is randomly distributed from the point view of the adversary $\mathcal{A}$ except with negligible probability of $\mathrm{Adv}_{\mathcal{A}}^{\text{ind-rka}}$. So we have that such ciphertexts will be rejected except with the probability of $\mathrm{Adv}_{\mathcal{A}}^{\text{ind-rka}} + 2^{-l_t}$.
  If $\tilde{\beta}/\tilde{\alpha} = w \mod \phi(N)$ the challenger $\mathcal{C}$ can compute:

$$w = \tilde{\beta}/\tilde{\alpha} = \mathrm{dlog}_T(\tilde{u}_2^{\phi(N)})/\mathrm{dlog}_T(\tilde{u}_1^{\phi(N)}).$$

Let ϵ_{dlg} be the probability that any adversary breaks the discrete logarithm assumption, we have that the probability that such cases happens is ϵ_{dlg}.

- $\tilde{\alpha} \neq 0, \tilde{\beta} = 0$ or $\tilde{\alpha} = 0, \tilde{\beta} \neq 0$: Similar as the case $\tilde{\beta}/\tilde{\alpha} \neq w \mod \phi(N)/4$ above, such ciphertexts will be rejected except with the probability of $\mathrm{Adv}_{\mathcal{A}}^{\text{ind-rka}} + 2^{-l_t}$.
- $\alpha' \neq 0, \beta' \neq 0$: If $\alpha'/\beta' \neq \alpha/\beta$, we have that $k = \alpha'(x_1^{hide} + \bar{x}_{i1}^{hide}) + \beta'(x_2^{hide} + \bar{x}_{i2}^{hide}) + \gamma' \mod N$ is linearly independent with equation (23). Hence $k \in Z_N$ is randomly distributed from the point view of $\mathcal{A}$, such ciphertexts will be rejected except with the probability of 2^{-l_N}.
  If $\alpha'/\beta' = \alpha/\beta \mod N$, let $\alpha' = \bar{r}\alpha \mod N, \beta' = \bar{r}\beta \mod N, \gamma' = \bar{r}(-\alpha x_{i1}^{hide} - \beta x_{i2}^{hide} + k^*) + \gamma \mod N$, we have:

  $$k = \bar{r}k^* + \gamma.$$

  According to the INT-RKA security of $\bar{\pi}$, such ciphertexts will be rejected except with the probability of $\mathrm{Adv}_{\mathcal{A}}^{\text{int-rka}}$.
- $\alpha' \neq 0, \beta' = 0$ or $\alpha' = 0, \beta' \neq 0$: Similar as the case of $\alpha'/\beta' \neq \alpha/\beta \mod N$, such ciphertexts will be rejected except with the probability of 2^{-l_N}.

According to the analysis above, we have that in Game 7:

$$\Pr[Bad] \leq \mathrm{Adv}_{\mathcal{A}}^{\text{ind-rka}} + \mathrm{Adv}_{\mathcal{A}}^{\text{int-rka}} + 2^{-l_t} + 2^{-l_N} + \epsilon_{dlg}$$

Hence we have:

$$\Pr[W_7] \leq \Pr[W_8] + \Pr[Bad]. \tag{24}$$

– **Game 9:** This game is exactly like Game 8, except that when responding to the key-dependent encryption query, the challenger $\mathcal{C}$ randomly chooses $k^*, \bar{k}^* \in Z_N$, computes e_λ^* and v_λ^* as follows:

$$s_\lambda^* \overset{R}{\leftarrow} Z_N, k_\lambda^* \leftarrow r_\lambda^* k^* + s_\lambda^* \mod N, e_\lambda^* \leftarrow (u_{\lambda 1}^{*-x_{i1}} u_{\lambda 2}^{*-x_{i2}}) T^{k_\lambda^*} \mod N^2,$$

$$\bar{k}_\lambda^* \leftarrow r_\lambda^* \bar{k}^* + s_\lambda^* \mod N, v_\lambda^* \leftarrow \bar{\pi}.\mathrm{E}_{\bar{k}_\lambda^*}(t_\lambda^* || \tilde{u}_{\lambda 1}^* || \tilde{u}_{\lambda 2}^* || \tilde{e}_\lambda^*).$$

Since all the decryption queries that $\tilde{\alpha} \neq 0$ or $\tilde{\beta} \neq 0$ or $\alpha' \neq 0$ or $\beta' \neq 0$ are rejected, we have that x_1^{hide} and x_2^{hide} are randomly distributed from the point view of $\mathcal{A}$ conditioned on the public key and the decryption oracle. In addition, when $(u_1 = u_{\lambda 1}^*, u_2 = u_{\lambda 2}^*, e = e_\lambda^*, v \neq v_\lambda^*)$ decryption queries are also rejected. Hence, the decryption oracle will not leak any information of k^*. According to equation (23), k^* is randomly distributed. So we have:

$$\Pr[W_8] \leq \Pr[W_9]. \tag{25}$$

According to the IND-RKA security of $\bar{\pi}$, the probability that $\mathcal{A}$ wins in Game 9 is:

$$\Pr[W_9] \leq 1/2 + \mathrm{Adv}_{\mathcal{A}}^{\text{ind-rka}}. \tag{26}$$

According to equations above we have:

$$\mathrm{AdvKDM}^{\mathrm{cca}}_{\mathcal{A},n} \leq 2\mathrm{Adv}^{\mathrm{iv2}}_{\mathcal{A}} + 2\mathrm{Adv}^{\text{int-rka}}_{\mathcal{A}} + 2\mathrm{Adv}^{\text{ind-rka}}_{\mathcal{A}} + \epsilon. \tag{27}$$

where $\epsilon = 2 \cdot 2^{-l_N} + 2^{-l_N/2} + 2^{-l_t} + \epsilon_{dlg}$.

This completes the proof of the theorem 2. □

5 Conclusion

We propose an efficient KDM-CCA secure public key encryption scheme with respect to affine functions by enhancing an IND-CCA2 secure hybrid encryption scheme based on the high entropy hash proof system. Our main idea is to divide the entropy of the private key into two parts: one part is embedded into the authentication tag, the other part is used to protect an original key for the authenticated encryption scheme. To hide the authentication tags from the adversary perfectly, we use an RKA secure authenticated encryption scheme and derive the keys from affine functions of the original key.

Compared with Hofheinz's scheme [33], our new scheme is simpler and more efficient. In addition, our new scheme achieves KDM-CCA security with respect to affine functions while Hofheinz's scheme only achieves CIRC-CCA security.

References

1. Abdalla, M., Benhamouda, F., Passelègue, A., Paterson, K.G.: Related-key security for pseudorandom functions beyond the linear barrier. In: Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I. pp. 77–94 (2014)
2. Alperin-Sheriff, J., Peikert, C.: Circular and KDM security for identity-based encryption. In: Public Key Cryptography - PKC 2012 - 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012. Proceedings. pp. 334–352 (2012)
3. Applebaum, B.: Key-dependent message security: Generic amplification and completeness. In: Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings. pp. 527–546 (2011)
4. Applebaum, B., Cash, D., Peikert, C., Sahai, A.: Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In: Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings. pp. 595–618 (2009)
5. Applebaum, B., Harnik, D., Ishai, Y.: Semantic security under related-key attacks and applications. In: Innovations in Computer Science - ICS 2010, Tsinghua University, Beijing, China, January 7-9, 2011. Proceedings. pp. 45–60 (2011)
6. Backes, M., Dürmuth, M., Unruh, D.: OAEP is secure under key-dependent messages. In: Advances in Cryptology - ASIACRYPT 2008, 14th International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, Australia, December 7-11, 2008. Proceedings. pp. 506–523 (2008)

7. Backes, M., Pfitzmann, B., Scedrov, A.: Key-dependent message security under active attacks - brsim/uc-soundness of dolev-yao-style encryption with key cycles. Journal of Computer Security 16(5), 497–530 (2008)
8. Barak, B., Haitner, I., Hofheinz, D., Ishai, Y.: Bounded key-dependent message security. In: Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010. Proceedings. pp. 423–444 (2010)
9. Bellare, M., Cash, D.: Pseudorandom functions and permutations provably secure against related-key attacks. In: Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings. pp. 666–684 (2010)
10. Bellare, M., Cash, D., Miller, R.: Cryptography secure against related-key attacks and tampering. In: Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings. pp. 486–503 (2011)
11. Bellare, M., Keelveedhi, S.: Authenticated and misuse-resistant encryption of key-dependent data. In: Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings. pp. 610–629 (2011)
12. Bellare, M., Kohno, T.: A theoretical treatment of related-key attacks: Rka-prps, rka-prfs, and applications. In: Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings. pp. 491–506 (2003)
13. Bellare, M., Paterson, K.G., Thomson, S.: RKA security beyond the linear barrier: Ibe, encryption and signatures. In: Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings. pp. 331–348 (2012)
14. Biham, E.: New types of cryptoanalytic attacks using related keys (extended abstract). In: Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings. pp. 398–409 (1993)
15. Biham, E., Shamir, A.: Differential fault analysis of secret key cryptosystems. In: Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings. pp. 513–525 (1997)
16. Black, J., Rogaway, P., Shrimpton, T.: Encryption-scheme security in the presence of key-dependent messages. In: Selected Areas in Cryptography, 9th Annual International Workshop, SAC 2002, St. John's, Newfoundland, Canada, August 15-16, 2002. Revised Papers. pp. 62–75 (2002)
17. Böhl, F., Davies, G.T., Hofheinz, D.: Encryption schemes secure under related-key and key-dependent message attacks. In: Public-Key Cryptography - PKC 2014 - 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, Argentina, March 26-28, 2014. Proceedings. pp. 483–500 (2014)
18. Boneh, D., DeMillo, R.A., Lipton, R.J.: On the importance of checking cryptographic protocols for faults (extended abstract). In: Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 11-15, 1997, Proceeding. pp. 37–51 (1997)

19. Boneh, D., Halevi, S., Hamburg, M., Ostrovsky, R.: Circular-secure encryption from decision diffie-hellman. In: Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings. pp. 108–125 (2008)
20. Brakerski, Z., Goldwasser, S.: Circular and leakage resilient public-key encryption under subgroup indistinguishability - (or: Quadratic residuosity strikes back). In: Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings. pp. 1–20 (2010)
21. Brakerski, Z., Goldwasser, S., Kalai, Y.T.: Black-box circular-secure encryption beyond affine functions. In: Theory of Cryptography - 8th Theory of Cryptography Conference, TCC 2011, Providence, RI, USA, March 28-30, 2011. Proceedings. pp. 201–218 (2011)
22. Camenisch, J., Chandran, N., Shoup, V.: A public key encryption scheme secure against key dependent chosen plaintext and adaptive chosen ciphertext attacks. In: Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings. pp. 351–368 (2009)
23. Camenisch, J., Lysyanskaya, A.: An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In: Advances in Cryptology - EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding. pp. 93–118 (2001)
24. Canetti, R., Halevi, S., Katz, J.: Chosen-ciphertext security from identity-based encryption. In: Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings. pp. 207–222 (2004)
25. Cramer, R., Shoup, V.: Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In: Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings. pp. 45–64 (2002)
26. Damgård, I., Jurik, M.: A generalisation, a simplification and some applications of paillier's probabilistic public-key system. In: Public Key Cryptography, 4th International Workshop on Practice and Theory in Public Key Cryptography, PKC 2001, Cheju Island, Korea, February 13-15, 2001, Proceedings. pp. 119–136 (2001)
27. Galindo, D., Herranz, J., Villar, J.L.: Identity-based encryption with master key-dependent message security and leakage-resilience. In: Computer Security - ESORICS 2012 - 17th European Symposium on Research in Computer Security, Pisa, Italy, September 10-12, 2012. Proceedings. pp. 627–642 (2012)
28. Gentry, C.: Fully homomorphic encryption using ideal lattices. In: Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009. pp. 169–178 (2009)
29. Goldenberg, D., Liskov, M.: On related-secret pseudorandomness. In: Theory of Cryptography, 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010. Proceedings. pp. 255–272 (2010)
30. Goyal, V., O'Neill, A., Rao, V.: Correlated-input secure hash functions. In: Theory of Cryptography - 8th Theory of Cryptography Conference, TCC 2011, Providence, RI, USA, March 28-30, 2011. Proceedings. pp. 182–200 (2011)
31. Haitner, I., Holenstein, T.: On the (im)possibility of key dependent encryption. In: Theory of Cryptography, 6th Theory of Cryptography Conference, TCC 2009, San Francisco, CA, USA, March 15-17, 2009. Proceedings. pp. 202–219 (2009)

32. Halevi, S., Krawczyk, H.: Security under key-dependent inputs. In: Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, Alexandria, Virginia, USA, October 28-31, 2007. pp. 466–475 (2007)
33. Hofheinz, D.: Circular chosen-ciphertext security with compact ciphertexts. In: Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings. pp. 520–536 (2013)
34. Hofheinz, D., Unruh, D.: Towards key-dependent message security in the standard model. In: Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings. pp. 108–126 (2008)
35. Jia, D., Li, B., Lu, X., Mei, Q.: Related key secure PKE from hash proof systems. In: Advances in Information and Computer Security - 9th International Workshop on Security, IWSEC 2014, Hirosaki, Japan, August 27-29, 2014. Proceedings. pp. 250–265 (2014), http://dx.doi.org/10.1007/978-3-319-09843-2_19
36. Jia, D., Lu, X., Li, B., Mei, Q.: RKA secure PKE based on the DDH and HR assumptions. In: Provable Security - 7th International Conference, ProvSec 2013, Melaka, Malaysia, October 23-25, 2013. Proceedings. pp. 271–287 (2013)
37. Kiltz, E., Pietrzak, K., Stam, M., Yung, M.: A new randomness extraction paradigm for hybrid encryption. In: Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings. pp. 590–609 (2009)
38. Knudsen, L.R.: Cryptanalysis of LOKI91. In: Advances in Cryptology - AUSCRYPT '92, Workshop on the Theory and Application of Cryptographic Techniques, Gold Coast, Queensland, Australia, December 13-16, 1992, Proceedings, pp. 196–208 (1992)
39. Lu, X., Li, B., Jia, D.: Related-key security for hybrid encryption. In: Information Security - 17th International Conference, ISC 2014, Hong Kong, China, October 12-14, 2014. Proceedings. pp. 19–32 (2014), http://dx.doi.org/10.1007/978-3-319-13257-0_2
40. Malkin, T., Teranishi, I., Yung, M.: Efficient circuit-size independent public key encryption with KDM security. In: Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings. pp. 507–526 (2011)
41. Naor, M., Yung, M.: Public-key cryptosystems provably secure against chosen ciphertext attacks. In: Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, May 13-17, 1990, Baltimore, Maryland, USA. pp. 427–437 (1990)
42. Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In: Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding. pp. 223–238 (1999)
43. Wee, H.: Public key encryption against related key attacks. In: Public Key Cryptography - PKC 2012 - 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012. Proceedings. pp. 262–279 (2012)