RKA-KDM secure encryption from public-key encryption

Florian Böhl[*a], Gareth T. Davies[†b] and Dennis Hofheinz[‡a]

[a]Karlsruhe Institute of Technology (KIT), Department of Informatics,
Am Fasanengarten 5, 76131 Karlsruhe, Germany.
{florian.boehl,dennis.hofheinz}@kit.edu
[b]Department of Computer Science, University of Bristol,
Merchant Venturers Building, Woodland Road,
Bristol, BS8 1UB, United Kingdom.
gareth.davies@bristol.ac.uk

October 10, 2013

Abstract

We construct secret-key encryption (SKE) schemes that are secure against related-key attacks *and* in the presence of key-dependent messages (RKA-KDM secure). We emphasize that RKA-KDM security is not merely the conjunction of individual security properties, but covers attacks in which ciphertexts of key-dependent messages under related keys are available. Besides being interesting in their own right, RKA-KDM secure schemes allow to garble circuits with XORs very efficiently (Applebaum, TCC 2013). Until now, the only known RKA-KDM secure SKE scheme (due to Applebaum) is based on the LPN assumption. Our schemes are based on various other computational assumptions, namely DDH, LWE, QR, and DCR.

We abstract from Applebaum's construction and proof, and formalize three generic technical properties that imply RKA-KDM security: one property is IND-CPA security, and the other two are the existence of suitable oracles that produce ciphertexts under related keys, resp. of key-dependent messages. We then give simple SKE schemes that achieve these properties. Our constructions are variants of known KDM-secure public-key encryption schemes. To additionally achieve RKA security, we isolate suitable homomorphic properties of the underlying schemes in order to simulate ciphertexts under related keys in the security proof.

From a conceptual point of view, our work provides a generic and extensible way to construct encryption schemes with multiple special security properties.

Keywords: related key attacks, key-dependent message security, garbled circuits.

[*]Supported by MWK grant "MoSeS".
[†]This author was partially supported by an EPSRC DTA award. Work partially conducted while visiting KIT.
[‡]Supported by DFG grant GZ HO 4534/2-1.

1 Introduction

Motivation and overview. The standard notion of security for secret-key encryption (SKE) is indistinguishability of ciphertexts (short: IND-CPA or IND-CCA, depending on whether passive or active attacks are considered). However, in certain applications, ciphertext indistinguishability is not sufficient. For instance, in harddisk encryption, encryptions of the secret key itself naturally occur (see [22]). Security in the presence of such key-dependent messages (KDM security [21]) is not implied by IND-CPA or IND-CCA security [21, 1]. There are numerous other specialized notions of encryption scheme security, such as security under related-key attacks (RKAs [7]), leakage-resilience [32, 26], security under bad randomness [10], security under selective openings [11], and others.

In this paper, we consider two such specialized notions of security for SKE schemes in a combined fashion. In particular, we will derive SKE schemes that are secure in the presence of key-dependent messages encrypted under related keys. This notion, dubbed RKA-KDM security and already considered by Applebaum [3] (as RK-KDM security), combines the notions of KDM and RKA security, but is more than just their conjunction. RKA-KDM secure SKE schemes are of course suitable for all applications in which RKA or KDM security is required. In fact, there are even applications that explicitly require the combined RKA-KDM notion: Applebaum [3] uses RKA-KDM secure SKE schemes in a garbled circuit construction in which XOR gates can be garbled for free (in the sense that XOR gates require no explicit encryption whatsoever). Besides, "aggregating" security properties as in RKA-KDM security may eventually lead to more "ideal" and universally useful security notions and encryption schemes.

RKA and KDM security. To give more details, we first recall the definitions of IND-CPA, RKA, and KDM security. In a nutshell, an SKE scheme has indistinguishable ciphertexts (or, is IND-CPA secure [27][1]), if no efficient adversary $\mathcal{A}$ can tell apart whether it is interacting with an oracle Real, or with an oracle Fake. Here, upon input M, oracle Real returns an encryption $\mathsf{E}_k(M)$ of M, while Fake returns an encryption $\mathsf{E}_k(0^{|M|})$ of a zero-string of the same length. (In other words, $\mathcal{A}$ is asked to tell authentic encryptions from encryptions of meaningless messages of the same length.)

For security under key-dependent messages (KDM security [21]), we require the same, except that messages are now functions in the secret key. That is, upon input a function ψ, Real returns $\mathsf{E}_k(\psi(k))$, and Fake returns $\mathsf{E}_k(0^{|\psi(k)|})$. Depending on the class of allowed functions Ψ, there are many constructions of KDM-secure encryption schemes from various computational assumptions, e.g. [21, 28, 30, 22, 5, 25, 6, 23, 24, 31, 8, 12, 4, 29]. However, most of these works follow the design principle of Boneh et al. [22] (henceforth BHHO). Namely, it should be publicly possible (or at least given some "harmless" extra information) to construct key-dependent encryptions from regular ones. Intuitively, if this is the case, then clearly the presence of key-dependent encryptions is no more harmful than the presence of "regular", key-independent encryptions.

For security under related-key attacks (RKA security [9]), we again require the same as for IND-CPA security, except that an adversary $\mathcal{A}$ now specifies a function φ on secret keys alongside each message M to be encrypted. Real then returns an encryption $\mathsf{E}_{\varphi(k)}(M)$ of M under the related key $\varphi(k)$, and Fake returns $\mathsf{E}_{\varphi(k)}(0^{|M|})$. RKA security draws its motivation primarily from the wide range of *attacks* that are known in this setting, e.g. [14, 15, 16, 17, 19, 18, 20]. There are also a number of constructions of RKA secure schemes, e.g. [7, 13, 33, 3]. As with KDM security, the main idea is to generate encryptions under related keys from "regular" encryptions.

RKA-KDM security. It is of course easy to combine RKA and KDM security into a combined notion, which we call RKA-KDM security here. Concretely, RKA-KDM security is defined like IND-CPA security above, only that an adversary supplies functions φ and ψ along with the

[1] In the following, for ease of exposition, we describe a modified but equivalent version of IND-CPA security.

message M to be encrypted. Then, Real returns $\mathsf{E}_{\varphi(k)}(\psi(k))$, and Fake returns $\mathsf{E}_{\varphi(k)}(0^{|\psi(k)|})$. This notion has already been defined by Applebaum [3] (dubbed RK-KDM security there), who used RKA-KDM secure schemes to garble circuits with XOR gates in a very elegant and efficient way. As a proof of concept, Applebaum also constructed an RKA-KDM secure encryption scheme, starting from the KDM-secure scheme of Applebaum et al. [5] based on the LPN assumption. (Along the way, he also shows that RKA-KDM security is strictly stronger than the conjunction of RKA and KDM security.) Currently, no further RKA-KDM secure schemes are known.

Our contribution. In this work, we provide a generic framework to construct RKA-KDM secure encryption schemes, and we instantiate this framework under several computational assumptions. In particular, we provide RKA-KDM secure schemes from the decisional Diffie-Hellman (DDH), learning with errors (LWE), quadratic residuosity and decisional Diffie-Hellman (QR+DDH)[2], and decisional composite residuosity (DCR) assumptions. While our constructions support KDM and RKA functions in the "natural domain" of the respective secret keys, not all of them can be directly used in the application of Applebaum [3]. However, we present schemes that are compatible with [3] from the DDH, the LWE, and the QR+DDH assumptions. (Interestingly, in case of the DDH and LWE assumptions, we can use the techniques of Barak et al. [6] to provide a suitable form of KDM security.)

Our approach. Based on an informal remark of Applebaum [3], Remark 3.6 in full version, we first reduce RKA-KDM security to three technical properties of the scheme in question:
(a) IND-CPA security in the usual sense,
(b) the existence of an oracle (that itself has access to an $\mathsf{E}_k(\cdot)$ oracle) that generates ciphertexts $\mathsf{E}_{\varphi(k)}(M)$ under related keys, and
(c) the existence of an oracle (with access to $\mathsf{E}_k(\cdot)$) that generates ciphertexts $\mathsf{E}_k(\psi(k))$ of key-dependent messages.

Intuitively, property (b) allows to reduce any RKA-KDM attack to a KDM attack, which in turn can be reduced (using (c)) to an IND-CPA attack. We note that it seems possible to add further oracles (e.g., for encryption queries with leakage) to achieve even stronger combined security notions from individual and isolated technical properties.

We then proceed to construct several RKA-KDM secure encryption schemes. Our constructions are slight variations of the known KDM-secure schemes from [22, 5, 6, 23, 31]. For these schemes, properties (a) and (c) already follow (with slight modifications) from the KDM security proofs of the underlying schemes. Showing property (b) then boils down to showing suitable homomorphic properties of the encryption, resp. decryption algorithm. We remark that in our case, achieving RKA security (with respect to the class of functions that allows XORs on key bits) is slightly more challenging than for the LPN-based KDM-scheme of [3]. Namely, since the scheme of [3] works over an algebraic structure of characteristic 2, an XOR can be implemented by an addition. (This is not the case for our schemes based on DDH, DCR, and LWE.)

Example: our DDH-based scheme. To give a taste of the proof, we outline our DDH-based scheme (which is based upon the DDH-based public-key encryption scheme from [22]). In this scheme, a ciphertext is of the form

$$C = (g_1^{r_1}, \ldots, g_\lambda^{r_\lambda}, g^M \cdot g_0),$$

where λ is the security parameter, g and the g_i are uniformly random generators of the underlying cyclic group, the r_i are uniformly random exponents, and $g_0 = \prod_{i\in[\lambda]}(g_i^{r_i})^{-k_i}$ for the secret key $k = (k_1, \ldots, k_\lambda) \in \{0,1\}^\lambda$. (In the original public-key encryption scheme from [22], all r_i are identical.)

[2]Similar to Hofheinz [29], we have to use the DDH assumption in the group of quadratic residues modulo N.

We show property (b) for functions of the form $\varphi_\Delta : \{0,1\}^\lambda \to \{0,1\}^\lambda$ with $\varphi_\Delta(k) = k \oplus \Delta$ for some $\Delta \in \{0,1\}^\lambda$. (This will be sufficient for the application in [3].) To show (b), we only need to show that any given ciphertext $C = \mathsf{E}_k(M)$ as above can be transformed into a ciphertext $C' = \mathsf{E}_{\varphi_\Delta(k)}(M)$. For simplicity, assume that $\Delta = (1, 0, \ldots, 0)$. In this case, it is easy to see that

$$C' = (1/g_1^{r_1}, g_2^{r_2}, \ldots, g_\lambda^{r_\lambda}, (g^M \cdot g_0) \cdot g_1^{r_1})$$

is a perfectly distributed encryption of M under key $k' = k \oplus \Delta$ (with randomness $r'_1 = -r_1$ and $r'_i = r_i$ for $i > 1$). This shows property (b) – the other properties follow as in [22].[3]

Our other constructions proceed similarly, starting from the schemes of Applebaum et al. [5], Barak et al. [6], Brakerski and Goldwasser [23], and Malkin et al. [31].

2 Preliminaries

Notation. For $n \in \mathbb{N}$, let $[n] := \{1, \ldots, n\}$. Throughout the paper, $\lambda \in \mathbb{N}$ denotes the security parameter. For a finite set $\mathcal{S}$, we denote by $s \leftarrow \mathcal{S}$ the process of sampling s uniformly from $\mathcal{S}$. For a distribution X, we denote by $x \leftarrow X$ the process of sampling x from X. For a probabilistic algorithm A, we denote with $y := A(x; r)$ the process of running A on input x and with randomness r, and assigning y the result. We let $\mathcal{R}_A$ denote the randomness space of A; we require $\mathcal{R}_A$ to be of the form $\mathcal{R}_A = \{0,1\}^\ell$. We write $y \leftarrow A(x)$ for $y \leftarrow A(x; r)$ with uniformly chosen $r \in \mathcal{R}_A$. If A's running time is polynomial in λ, then A is called probabilistic polynomial-time (PPT). For a real number x, let the floor function $\lfloor x \rfloor$ denote the largest integer not greater than x. For a vector $\mathbf{v}$, $\mathbf{v}_i$ denotes the ith element of $\mathbf{v}$.

Two sequences of random variables $X = (X_\lambda)_{\lambda \in \mathbb{N}}$ and $Y = (Y_\lambda)_{\lambda \in \mathbb{N}}$ are *computationally indistinguishable* (denoted $X \overset{c}{\approx} Y$) iff for any PPT algorithm D, the probability $\mathbf{Pr}\left[D(1^\lambda, X_\lambda) = 1\right] - \mathbf{Pr}\left[D(1^\lambda, Y_\lambda)\right]$ is negligible in λ. $X = (X_\lambda)_{\lambda \in \mathbb{N}}$ and $Y = (Y_\lambda)_{\lambda \in \mathbb{N}}$ are *statistically indistinguishable* (denoted $X \overset{s}{\approx} Y$) iff the same holds for any algorithm D with unbounded runtime.

SKE schemes. A secret-key encryption (SKE) scheme consists of four PPT algorithms $(\mathsf{Pg}, \mathsf{Kg}, \mathsf{E}, \mathsf{D})$. Parameter generation $\mathsf{Pg}(1^\lambda)$ outputs public parameters π for the scheme. Key generation $\mathsf{Kg}(\pi)$ outputs a (secret) key k. Encryption $\mathsf{E}_k(M)$ takes a key k and a message M, and outputs a ciphertext C. Decryption $\mathsf{Dec}_k(C)$ takes a key k and a ciphertext C, and outputs a message M or $\perp$ if decryption fails. For correctness, we stipulate $\mathsf{D}_k(C) = M$ for all M, all $k \leftarrow \mathsf{Kg}(\mathsf{Pg}(1^\lambda))$, and all $C \leftarrow \mathsf{E}_k(M)$.

Definition 1 ($\mathsf{RKA\text{-}KDM}[\Phi, \Psi]$ Security.)**.** *Let $\Sigma = (\mathsf{Pg}, \mathsf{Kg}, \mathsf{E}, \mathsf{D})$ be a symmetric encryption scheme, $\pi \leftarrow \mathsf{Pg}(1^\lambda)$ be public parameters and $b \leftarrow \{0,1\}$ be a bit chosen by the challenger. A key $k \leftarrow \mathsf{Kg}(\pi)$ is randomly chosen. Adversary $\mathcal{A}$ makes encryption queries by submitting $(\varphi \in \Phi, \psi \in \Psi)$ and receives a response from one of the following oracles, depending on the bit b.*

- *If $b = 1$, oracle Real_k takes as input (φ, ψ) and returns $C \leftarrow \mathsf{E}_{\varphi(k)}(\psi(k))$.*
- *If $b = 0$, oracle Fake_k takes as input (φ, ψ) and returns $C \leftarrow \mathsf{E}_{\varphi(k)}(0^{|\psi(k)|})$.*

Scheme Σ is $\mathsf{RKA\text{-}KDM}$ secure w.r.t. Φ and Ψ if for all PPT adversaries $\mathcal{A}$

$$\left|\mathsf{Pr}[\mathcal{A}^{\mathsf{Real}(\varphi,\psi)}(\pi) = 1] - \mathsf{Pr}[\mathcal{A}^{\mathsf{Fake}(\varphi,\psi)}(\pi) = 1]\right|$$

is a negligible function in λ.

[3] We note that our technical change to the scheme from [22] – namely, using *different* r_i – is not crucial to its security. Instead, choosing different r_i simplifies expressing the scheme in our framework, and in particular separating the KDM, RKA, and IND-CPA properties.

Throughout this paper each class of KDM functions Ψ implicitly contains constant functions $\psi_M(k) := M$ for all messages $M \in \mathcal{M}$ where $\mathcal{M}$ is the message space of the encryption scheme at hand.

Further security definitions. The standard definition of *RKA security* follows from restricting the KDM function class Ψ to constant functions, and the definition of *KDM security* follows from restricting the RKA function class Φ to the identity function. *IND-CPA security* follows from applying both of these restrictions at once.

2.1 A generic approach

In this section we prove that an SKE scheme Σ is $\mathsf{RKA\text{-}KDM}[\Phi, \Psi]$ secure if

- Σ is IND-CPA secure,
- there is a so called $\mathsf{RKA}[\Phi]$ oracle (defined below) for Σ that takes as input $\mathsf{E}_k(M)$ and RKA function $\varphi \in \Phi$, and returns something that is indistinguishable from $\mathsf{E}_{\varphi(k)}(M)$ without knowledge of the key k,
- there is a so called $\mathsf{KDM}[\Psi]$ oracle (defined below) for Σ that takes as input $\mathsf{E}_k(M)$ and KDM function $\psi \in \Psi$, and returns something that is indistinguishable from $\mathsf{E}_k(\psi(k))$ without knowledge of the key k (M is the constant part of ψ here).

Definition 2 ($\mathsf{RKA}[\Phi]$ oracle)**.** *Let $\Sigma = (\mathsf{Pg}, \mathsf{Kg}, \mathsf{E}, \mathsf{D})$ be a secret key encryption scheme with message space $\mathcal{M}$. We say that a function $\mathcal{F}_{\mathsf{RKA}[\Phi]}(\varphi, C)$ is an $\mathsf{RKA}[\Phi]$ oracle for Σ iff for all PPT adversaries $\mathcal{A}$ that make queries (φ, M) for $\varphi \in \Phi$ and $M \in \mathcal{M}$*

$$\left| \mathsf{Pr}\left[\mathcal{A}^{\mathcal{F}_{\mathsf{RKA}[\Phi]}(\varphi, \mathsf{E}_k(\cdot))}(\pi, k) = 1 : \pi \leftarrow \mathsf{Pg}(1^\lambda), k \leftarrow \mathsf{Kg}(\pi)\right] \right.$$
$$\left. - \mathsf{Pr}\left[\mathcal{A}^{\mathsf{E}_{\varphi(k)}(\cdot)}(\pi, k) = 1 : \pi \leftarrow \mathsf{Pg}(1^\lambda), k \leftarrow \mathsf{Kg}(\pi)\right] \right|$$

is a negligible function in λ.

Definition 3 ($\mathsf{KDM}[\Psi]$ oracle)**.** *Let $\Sigma = (\mathsf{Pg}, \mathsf{Kg}, \mathsf{E}, \mathsf{D})$ be a secret key encryption scheme with message space $\mathcal{M}$. We say that a function $\mathcal{F}_{\mathsf{KDM}[\Psi]}(\psi, C)$ is a $\mathsf{KDM}[\Psi]$ oracle for Σ iff for all PPT adversaries $\mathcal{A}$ that make queries ψ for $\psi \in \Psi$ (where M denotes the constant part of ψ)*

$$\left| \mathsf{Pr}\left[\mathcal{A}^{\mathcal{F}_{\mathsf{KDM}[\Psi]}(\psi, \mathsf{E}_k(M))}(\pi, k) = 1 : \pi \leftarrow \mathsf{Pg}(1^\lambda), k \leftarrow \mathsf{Kg}(\pi)\right] \right.$$
$$\left. - \mathsf{Pr}\left[\mathcal{A}^{\mathsf{E}_k(\psi(k))}(\pi, k) = 1 : \pi \leftarrow \mathsf{Pg}(1^\lambda), k \leftarrow \mathsf{Kg}(\pi)\right] \right|$$

is a negligible function in λ.

Note that for constant functions $\psi \in \Psi$ a sufficient behaviour of $\mathcal{F}_{\mathsf{KDM}[\Psi]}$ is to output the ciphertext it received without changes. All $\mathsf{KDM}[\Psi]$ oracles presented in this paper implicitly adopt this behaviour.

Theorem 1. *Let Σ be an SKE scheme that is IND-CPA secure, $\mathcal{F}_{\mathsf{RKA}[\Phi]}$ be an $\mathsf{RKA}[\Phi]$ oracle for Σ and $\mathcal{F}_{\mathsf{KDM}[\Psi]}$ be a $\mathsf{KDM}[\Psi]$ oracle for Σ. Then Σ is $\mathsf{RKA\text{-}KDM}[\Phi, \Psi]$ secure.*

Proof. We prove the theorem by a sequence of games.

Game 0 In Game 0 $\mathcal{A}$ plays the original $\mathsf{RKA\text{-}KDM}[\Phi, \Psi]$ experiment (see Definition 1).

Game 1 In Game 1, instead of computing $\mathsf{E}_{\varphi(k)}(\psi(k))$ the experiment computes $C_{\mathsf{KDM}} \leftarrow \mathsf{E}_k(\psi(k))$ and outputs $\mathcal{F}_{\mathsf{RKA}[\Phi]}(\varphi, C_{\mathsf{KDM}})$ to the adversary. This game is indistinguishable from Game 0 due to the indistinguishability of $\mathcal{F}_{\mathsf{RKA}[\Phi]}$ (see Definition 2).

Game 2 In Game 2, instead of computing $\mathsf{E}_k(\psi(k))$, the experiment computes $C_{\mathsf{CPA}} \leftarrow \mathsf{E}_k(M)$ where M is the constant part of ψ and sets $C_{\mathsf{KDM}} := \mathcal{F}_{\mathsf{KDM}[\Psi]}(\psi, C_{\mathsf{CPA}})$. Given a distinguisher $\mathcal{D}$ between this game and Game 1, we can construct an adversary $\mathcal{S}$, henceforth called simulator, on the indistinguishability of $\mathcal{F}_{\mathsf{KDM}[\Psi]}$. First, the simulator forwards the public parameters π to $\mathcal{D}$ and picks a bit $b \leftarrow \{0,1\}$. For $b = 1$ and each query (φ, ψ) from $\mathcal{D}$, the simulator queries its oracle for ψ and either gets a response $\mathcal{F}_{\mathsf{KDM}[\Psi]}(\psi_M, C_{\mathsf{CPA}})$ or $\mathsf{E}_k(\psi_M(k))$ (see Definition 3). It then applies $\mathcal{F}_{\mathsf{RKA}[\Phi]}$ with φ to the response and sends the result to $\mathcal{D}$. The responses to the queries of the simulator are that of Game 2 if itself gets responses of type $\mathcal{F}_{\mathsf{KDM}[\Psi]}(\psi_M, C_{\mathsf{CPA}})$ and that of Game 1 for responses of type $\mathsf{E}_k(\psi_M(k))$. Analogously for $b = 0$, where the simulator queries $0^{|\psi(k)|}$ instead of ψ. The advantage of $\mathcal{S}$ is that of $\mathcal{D}$ and must be negligible due to the indistinguishability $\mathcal{F}_{\mathsf{KDM}[\Psi]}$.

Game 3 In Game 3 we replace $C_{\mathsf{CPA}} \leftarrow \mathsf{E}_k(M)$ by $C_{\mathsf{CPA}} \leftarrow \mathsf{E}_k(0^{|M|})$. Analogously to the indistinguishability of Game 1 and Game 2, we can easily transform a distinguisher between this game and the previous game into an IND-CPA adversary for Σ.

We observe that the advantage of any PPT adversary in Game 3 is 0 since the behaviour of the oracle given to the adversary is is independent of the bit b picked by the experiment. This concludes our proof since Game 3 and Game 0 are indistinguishable. □

3 RKA-KDM-secure Encryption Schemes

3.1 Boneh et al. [22]

The PKE scheme of Boneh et al. [22] was the first construction provably KDM secure under standard assumptions. In this section we detail a SKE analogue of the 'basic' version of their scheme. We construct an $\mathsf{RKA}[\Phi]$ oracle and a $\mathsf{KDM}[\Psi]$ oracle for the scheme. The class of RKA functions Φ allows for XOR operations on the key while the class of KDM functions Ψ brings circular KDM security, i.e., encryptions of the secret key are possible (as in the original paper). The security of the scheme is based on the DDH assumption.

DDH assumption. The *decisional Diffie-Hellman (DDH) assumption* over a group $\mathbb{G}$ (that may depend on the security parameter λ) stipulates that

$$(g, g^x, g^y, g^{xy}) \quad \overset{c}{\approx} \quad (g, g^x, g^y, g^z),$$

where $g \leftarrow \mathbb{G}$ and $x, y, z \leftarrow [|\mathbb{G}|]$ are uniformly distributed.

For the sake of readability we introduce the scheme Σ'_{BHHO} with message space $\{0,1\}$. Canonical concatenation at the end will yield the scheme Σ_{BHHO} with message space $\{0,1\}^\lambda$.

The SKE scheme Σ'_{BHHO}. Let $\mathbb{G}$ be a group of prime order p and g be a generator of $\mathbb{G}$. The scheme Σ'_{BHHO} for $M \in \{0,1\}$ is defined as follows:

- $\mathsf{Pg}(1^\lambda)$ picks generators $g_1, \ldots, g_\lambda \leftarrow \mathbb{G} \setminus \{1\}$ and returns $\pi := (\mathbb{G}, g, g_1, \ldots, g_\lambda)$.
- $\mathsf{Kg}(\pi)$ returns a random bitstring $k \leftarrow \{0,1\}^\lambda$.
- $\mathsf{E}_k(M)$ picks $r_1, \ldots, r_\lambda \leftarrow \mathbb{Z}_p$. Sets $g_0 := \prod_{i \in [\lambda]} (g_i^{r_i})^{-k_i}$ and returns

$$C := (g_1^{r_1}, \ldots, g_\lambda^{r_\lambda}, g^M \cdot g_0) \in \mathbb{G}^{\lambda+1}.$$

- $\mathsf{D}_k(C)$ parses C as $(x_1, \ldots, x_\lambda, y)$. Computes $\tilde{M} := y \cdot \prod_{i \in [\lambda]} x_i^{k_i}$. Returns 0 if $\tilde{M} = 1$, returns 1 if $\tilde{M} = g$, otherwise returns $\perp$.

The $\mathsf{RKA}[\Phi]$ oracle. For the concrete class of RKA functions

$$\Phi := \{\varphi_\Delta : \{0,1\}^\lambda \to \{0,1\}^\lambda, k \mapsto k \oplus \Delta : \Delta \in \{0,1\}^\lambda\}$$

we find an $\mathsf{RKA}[\Phi]$ oracle $\mathcal{F}_{\mathsf{RKA}[\Phi]}$ for Σ'_{BHHO} as follows: Given a ciphertext $C = (x_1, \ldots, x_\lambda, y)$ and a function φ_Δ it outputs

$$C' := (x'_1, \ldots, x'_\lambda, y') := (x_1^{(-1)^{\Delta_1}}, \ldots, x_\lambda^{(-1)^{\Delta_\lambda}}, y \cdot \prod_{i\in[\lambda]} x_i^{\Delta_i})$$

To understand this better we assume that C is an honestly generated ciphertext (as it will be in the indistinguishability experiment for $\mathcal{F}_{\mathsf{RKA}[\Phi]}$). Then we have $y = g^M \cdot \prod_{i\in[\lambda]} x_i^{-k_i}$. We observe

$$y' = g^M \cdot \prod_{i\in[\lambda]} x_i^{-k_i} \cdot \prod_{i\in[\lambda]} x_i^{\Delta_i} = g^M \cdot \prod_{i\in[\lambda]} {x'_i}^{(-1)^{\Delta_i}(-k_i+\Delta_i)} \overset{(*)}{=} g^M \cdot \prod_{i\in[\lambda]} {x'_i}^{-(k_i\oplus\Delta_i)}$$

and $(*)$ since

$$(-1)^{\Delta_i}(-k_i + \Delta_i) = \left\{ \begin{array}{r} -k_i \text{ if } \Delta_i = 0 \\ -(1-k_i) \text{ if } \Delta_i = 1 \end{array} \right\} = -(k_i \oplus \Delta_i)$$

Therefore C' decrypts to M under key $k \oplus \Delta$.

Lemma 2. *$\mathcal{F}_{\mathsf{RKA}[\Phi]}$ is an $\mathsf{RKA}[\Phi]$ oracle in the sense of Definition 2.*

Proof. It is easy to see that the distributions of $\mathcal{F}_{\mathsf{RKA}[\Phi]}(\varphi_\Delta, \mathsf{E}_k(M))$ and $\mathsf{E}_{k\oplus\Delta}(M)$ are perfectly indistinguishable (even for someone knowing k and Δ): The x'_i just look like $r'_i = (-1)^{\Delta_i} r_i$ was used as randomness for the ith component (which yields the same distribution) and we have $y' = g^M \cdot \prod_{i\in[\lambda]} (x'_i)^{-(k_i\oplus\Delta_i)}$. □

The $\mathsf{KDM}[\Psi]$ oracle. For the class of KDM functions

$$\Psi := \{\psi_i : \{0,1\}^\lambda \to \{0,1\}, k \mapsto k_i : i \in [\lambda]\}$$

we find the following $\mathsf{KDM}[\Psi]$ oracle $\mathcal{F}_{\mathsf{KDM}[\Psi]}$ for Σ'_{BHHO}: Given a function ψ_i and an honestly generated ciphertext of 0 (the message part of ψ_i is 0) $C = (x_1, \ldots, x_\lambda, y)$ it outputs

$$C' := (x'_1, \ldots, x'_\lambda, y') := (x_1, \ldots, x_{i-1}, x_i \cdot g, x_{i+1}, \ldots, x_\lambda, y)$$

We check that this ciphertext decrypts to k_i:

$$y \cdot \prod_{j\in[\lambda]} {x'_j}^{k_j} \overset{(*)}{=} y \cdot \left(\prod_{j\in[\lambda]} {x_j}^{k_j}\right) \cdot g^{k_i} = \left(\prod_{j\in[\lambda]} {x_j}^{-k_j} \cdot \prod_{j\in[\lambda]} {x_j}^{k_j}\right) \cdot g^{k_i} = g^{k_i}$$

$(*)$ since $x'_i = x_i \cdot g$ and $x'_j = x_j$ for $j \in [\lambda] \setminus \{i\}$.

Lemma 3. *$\mathcal{F}_{\mathsf{KDM}[\Psi]}$ is an $\mathsf{KDM}[\Psi]$ oracle in the sense of Definition 3.*

Proof. We show that the distributions of $\mathcal{F}_{\mathsf{KDM}[\Psi]}(\psi_i, \mathsf{E}_k(0))$ and $\mathsf{E}_k(\psi_i(k))$ are perfectly indistinguishable. First, we observe that $x_i = g_i^{r_i}$ and $g = g_i^\alpha$ for $\alpha := \log_{g_i}(g)$, i.e., $x'_i = g_i^{r_i+\alpha}$. Furthermore we have $y = \prod_{j\in[\lambda]} {x_j}^{-k_j} = \prod_{j\in[\lambda]} {x_j}^{-k_j} g^{-k_i} g^{k_i} = \prod_{j\in[\lambda]} {x'_j}^{-k_j} g^{k_i}$. Hence the output of the oracle looks like a normal encryption of k_i where $r_i + \alpha$ was used as randomness in the ith component. □

IND-CPA security.

Lemma 4. *The SKE scheme Σ'_{BHHO} is IND-CPA secure if DDH is hard over the underlying group $\mathbb{G}$.*

Proof. Intuitively, we first use the hardness of DDH over $\mathbb{G}$ to collapse the randomness used by the encryption oracle to one random exponent per ciphertext, so instead of $r_1, \ldots, r_\lambda$ all generators are taken to the same random exponent r. This modified scheme is the 'basic' version of [22] with a smaller message space. We can then simply reduce security to the IND-CPA security of Boneh et al's scheme.

More concretely, we prove the lemma with the following sequence of games.

Game 0 In Game 0 $\mathcal{A}$ plays the original IND-CPA experiment.

Game 1 to **Game** $\lambda - 1$ form a hybrid argument to collapse the randomness used by the encryption oracle. In hybrid i ($i \in [\lambda - 1]$) we pick the same randomness for the first $i + 1$ components of the ciphertext. I.e., the format of a ciphertext output by the encryption oracle in game i is

$$\left(g_1^r, \ldots, g_{i+1}^r, g_{i+2}^{r_{i+2}}, \ldots, g_\lambda^{r_\lambda}, g^M \cdot \left(\prod_{i \in [i+1]} g_i^{-rk_i} \right) \left(\prod_{i \in [\lambda] \setminus [i+1]} g_i^{-r_i k_i} \right) \right)$$

Analysis. Each of the game hops above is indistinguishable due to the hardness of DDH over $\mathbb{G}$. The simulation for a hop from Game $i-1$ to Game i ($i \in [\lambda - 1]$) works as follows: The simulator $\mathcal{S}$ gets a DDH challenge $(g, X := g^x, Y := g^y, Z := g^{xy/z})$. For $j \in [\lambda] \setminus \{i+1\}$ it picks $\alpha_j \leftarrow \mathbb{Z}_p$, sets $g_j := g^{\alpha_j}$ and $g_{i+1} := X$. Subsequently it picks a key $k \leftarrow \{0,1\}^\lambda$ and sends the public parameters $\pi := (\mathbb{G}, g, g_1, \ldots, g_\lambda)$ to $\mathcal{A}$. If $\mathcal{A}$ requests an encryption of message M, $\mathcal{S}$ picks randomness $r, r_{i+2}, \ldots, r_\lambda, a, b \leftarrow \mathbb{Z}_p$ and sets $\hat{Y} := g^a \cdot Y^b$ and $\hat{Z} := X^a \cdot Z^b$ to re-randomize the DDH challenge. Finally, $\mathcal{S}$ sends

$$\left(\hat{Y}^{r\alpha_1}, \ldots, \hat{Y}^{r\alpha_i}, \hat{Z}^r, g_{i+2}^{r_{i+2}}, \ldots, g^M \cdot g_0 \right)$$

to the adversary where g_0 is computed as usual ($\mathcal{S}$ knows k). If $Z = g^z$, the output of $\mathcal{S}$ looks like that of game $i-1$, otherwise (for $Z = g^{xy}$) it looks like that of game i. Any PPT distinguisher between those games with non-negligible advantage can thus be used to break DDH.

Finally, only one fresh random exponent is used for each ciphertext in game $\lambda - 1$. The output now looks like that of the BHHO (public key) cryptosystem with message space $\{g^0, g^1\}$.

In **Game** λ, we replace the message with 0. The indistinguishability of game $\lambda - 1$ and game λ can be reduced to the IND-CPA security of Boneh et al's original scheme in a straightforward way (using the generators from the public key as public parameters). Hence IND-CPA security of Σ'_{BHHO} follows. □

The full scheme Σ_{BHHO}. Finally, we assemble the SKE scheme Σ_{BHHO} from λ instances of Σ'_{BHHO} that use the same public parameters π and the same key k. A ciphertext under Σ_{BHHO} is a matrix from $\mathbb{G}^{\lambda \times (\lambda+1)}$ where each row is an instance of Σ'_{BHHO} (using π and key k). To encrypt a message $M \in \{0,1\}^\lambda$ under key k we encrypt M_i in row i (while picking fresh randomness r_i, $i \in [\lambda]$ for each row). Decryption also works row-wise.

For the $\mathsf{RKA}[\Phi]$ oracle we apply $\mathcal{F}_{\mathsf{RKA}[\Phi]}$ to each row. The class of KDM functions Ψ changes to

$$\Psi := \{\psi_{\mathbf{i}} : \{0,1\}^\lambda \to \{0,1\}^\lambda, k \mapsto (k_{\mathbf{i}_1}, \ldots, k_{\mathbf{i}_\lambda}) : \mathbf{i} \in [\lambda]^\lambda\}$$

I.e., each bit of the message can be an arbitrarily picked key bit. For the $\mathsf{KDM}[\Psi]$ oracle provided with function $\psi_{\mathbf{i}}$, we apply $\mathcal{F}_{\mathsf{KDM}[\Psi']}$ with function $\psi_{\mathbf{i}_j} \in \Psi'$ to the jth row of the ciphertext

where Ψ' is the class of KDM functions for Σ'_{BHHO}. Since the oracles work row-wise it is easy to check that the indistinguishability results from Lemma 2 and Lemma 2 carry over to Σ_{BHHO}. Analogously for the IND-CPA security of Σ_{BHHO}. Finally, by Theorem 1, we get

Theorem 5. *The SKE scheme Σ_{BHHO} is $\mathsf{RKA\text{-}KDM}[\Phi, \Psi]$ secure (for Φ and Ψ as defined above in this section) if DDH is hard over the underlying group $\mathbb{G}$.*

3.2 Applebaum et al. [5]

In this section, we present a secret-key version of the PKE scheme of Applebaum et al. [5] and prove it RKA-KDM secure. For compatibility with Applebaum's application, however, we slightly change the space of secret keys from $\mathbb{Z}_p^m$ to $\{0,1\}^m$. Our RKA and KDM oracles allow encryptions under keys $k \oplus \Delta$ (for arbitrary $\Delta \in \{0,1\}^m$) of arbitrary components of the secret key. Security is based on the LWE assumption.

For ease of exposition, we do not detail the choices of the following parameters – these can occur as in [5] (with adaptations as in [2] due to the different choice of secret key). Let q be a polynomial in the security parameter λ, and let $m > n$ be integers (that may also depend on λ). By χ, we denote a (discretized Gaussian) error distribution with suitable parameters over $\mathbb{Z}_q$.

LWE assumption. Let $\mathbf{s} \in \mathbb{Z}_q^n$ be uniformly chosen. Let $\mathsf{LWE}_{\mathbf{s}}$ be the oracle that (on trivial input) returns $(\mathbf{a}, \langle \mathbf{a}; \mathbf{s} \rangle + x) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ for freshly chosen $\mathbf{a} \leftarrow \mathbb{Z}_q^n$ and $x \leftarrow \chi$. Let RND be the oracle that returns a freshly and independently chosen $(\mathbf{a}, \mathbf{b}) \leftarrow \mathbb{Z}_q^n \times \mathbb{Z}_q$. The LWE assumption states that oracle access to $\mathsf{LWE}_{\mathbf{s}}$ is computationally indistinguishable from oracle access to RND.

Applebaum et al. [5] show that the LWE assumption over $\mathbb{Z}_q = \mathbb{Z}_{p^2}$ and with $\mathbf{s} \leftarrow \mathbb{Z}_p^n$ is equivalent to the LWE assumption as above (for $q = p$). Furthermore, Akavia et al. [2] show that the LWE assumption with $\mathbf{s} \leftarrow \{0,1\}^n$ is implied by the LWE assumption as above (for different parameters of n, m). In the following, we will consider $q = p^2$ and $\mathbf{s} \in \{0,1\}^n$. Furthermore, for $x \in \mathbb{R}$, we write $\lceil x \rfloor_p := \lceil x + 1/2 \rceil \bmod p$ for the nearest integer to x modulo p.

The SKE scheme Σ'_{ACPS}. The scheme Σ'_{ACPS} (with $M \in \mathbb{Z}_p$) is defined as follows:

- $\mathsf{Pg}(1^\lambda)$ returns the empty bitstring.
- $\mathsf{Kg}(\pi)$ returns a random bitstring $k := \mathbf{s} \leftarrow \{0,1\}^m$.
- $\mathsf{E}_k(M)$ picks $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$ and $\mathbf{r}, \mathbf{x} \leftarrow \chi^m$, and returns
  $$C := (\mathbf{A} \cdot \mathbf{r}, -(\mathbf{s}^T \cdot \mathbf{A} + \mathbf{x}^T) \cdot \mathbf{r} + p \cdot M) = (\mathbf{A} \cdot \mathbf{r}, -\mathbf{s}^T \cdot \mathbf{A} \cdot \mathbf{r} + \langle \mathbf{x}; \mathbf{r} \rangle + p \cdot M) \in \mathbb{Z}_q^m \times \mathbb{Z}_q$$
- $\mathsf{D}_k(C)$ parses $C =: (\mathbf{y}, z)$ and computes and returns $M := \lceil (\langle \mathbf{s}; \mathbf{y} \rangle + z)/p \rfloor_p$.

Compared to the PKE scheme of [5], we choose $\mathbf{s}$ slightly differently, and also choose different $\mathbf{A}, \mathbf{x}$ upon each encryption. We note that correctness holds only with overwhelming probability over the choice of $\mathbf{r}$ and $\mathbf{x}$. In particular, $|\langle \mathbf{x}; \mathbf{r} \rangle| < p/2$ with overwhelming probability.

The $\mathsf{RKA}[\Phi]$ oracle. For the concrete class of RKA functions

$$\Phi := \{\varphi_\Delta : \{0,1\}^m \to \{0,1\}^m, k \mapsto k \oplus \Delta : \Delta \in \{0,1\}^m\},$$

we find an $\mathsf{RKA}[\Phi]$ oracle $\mathcal{F}_{\mathsf{RKA}[\Phi]}$ for Σ'_{ACPS} as follows: Given a ciphertext $C = (\mathbf{y}, z)$ and a function φ_Δ, it outputs

$$C' := (\mathbf{y}', z') \qquad \text{with} \qquad \mathbf{y'}_i = (-1)^{\Delta_i} \mathbf{y}_i \quad \text{and} \quad z' = z + \sum_{i \in [m]} \Delta_i \mathbf{y}_i$$

As with the BHHO scheme, a quick calculation shows that C' is a perfectly distributed ciphertext of M under $k \oplus \Delta$. Thus:

Lemma 6. *$\mathcal{F}_{\mathsf{RKA}[\Phi]}$ is an $\mathsf{RKA}[\Phi]$ oracle in the sense of Definition 2.*

The $\mathsf{KDM}[\Psi]$ oracle. For the class of KDM functions

$$\Psi := \{\psi_i : \{0,1\}^m \to \{0,1\}, k \mapsto k_i : i \in [m]\}$$

and following [5], we find the following $\mathsf{KDM}[\Psi]$ oracle $\mathcal{F}_{\mathsf{KDM}[\Psi]}$ for Σ'_{ACPS}: Given a function ψ_i and an honestly generated ciphertext $C = (\mathbf{y}, z)$ of $M = 0$, it outputs

$$C' := (\mathbf{y} + \mathbf{e}_i, z) \qquad \text{for the } i\text{-th unit vector } \mathbf{e}_i.$$

We check that this ciphertext decrypts to k_i:

$$\begin{aligned}\mathsf{D}_k(C') = \lceil(\langle \mathbf{s}; \mathbf{y} + \mathbf{e}_i\rangle + z)/p\rfloor_p = \lceil(\langle \mathbf{s}; \mathbf{y}\rangle + \mathbf{s}_i + z)/p\rfloor_p \\ = \lceil(\mathbf{s}^T\mathbf{A}\mathbf{r} + \mathbf{s}_i + z)/p\rfloor_p = \lceil(\mathbf{s}_i + \langle \mathbf{x}; \mathbf{r}\rangle)/p\rfloor_p, = \mathbf{s}_i.\end{aligned}$$

In fact, it is easy to see that ciphertexts C' as produced by $\mathcal{F}_{\mathsf{KDM}[\Psi]}$ are perfectly distributed ciphertexts of $M = \mathbf{s}_i$. We get:

Lemma 7. *$\mathcal{F}_{\mathsf{KDM}[\Psi]}$ is a $\mathsf{KDM}[\Psi]$ oracle in the sense of Definition 3.*

IND-CPA security.

Lemma 8. *The SKE scheme Σ'_{ACPS} is IND-CPA secure if the LWE assumption holds for the respective parameters.*

Sketch. Our scheme is essentially the same as that of [5], only with a different distribution of $\mathbf{s}$ (for which, by [2], the LWE assumption is implied by the "regular" LWE assumption). Hence, we only provide a short overview over the proof of [5].

First, we substitute all vectors $\mathbf{s}^T\mathbf{A} + \mathbf{x}^T$ used to handle encryption queries with independently and uniformly random vectors $\mathbf{u}^T$. This step can be justified by applying the LWE assumption.

Next, we observe that now encryption has become lossy, in the sense that ciphertexts are statistically (almost) independent of the underlying message. Indeed, by our choice of $m > n$, given $\mathbf{A}\mathbf{r}$, the vector $\mathbf{r}$ still has significant min-entropy. Thus, the value $\langle \mathbf{u}; \mathbf{r}\rangle$ used to pad the encrypted message looks (almost) uniformly and independently distributed. At this point, $\mathcal{A}$'s advantage to distinguish real from fake encryptions is statistically close to zero, and IND-CPA security follows. □

The full scheme Σ_{ACPS}. As in the BHHO setting, we can construct the full scheme Σ_{ACPS} with message space $\mathbb{Z}_p^m$ from m instances of Σ'_{ACPS} that use the same public parameters and key in a straightforward manner.

Likewise, by transferring Lemma 6, Lemma 7 and Lemma 8 from Σ'_{ACPS} to Σ_{ACPS} and by Theorem 1, we get

Theorem 9. *The SKE scheme Σ_{ACPS} is RKA-$\mathsf{KDM}[\Phi, \Psi]$ secure (for Φ and Ψ as defined above in this section) if the LWE assumption holds for the respective parameters.*

3.3 Brakerski-Goldwasser [23]

In this section we consider the encryption scheme of Brakerski and Goldwasser [23], modified to the symmetric setting. The KDM security of the original (public-key) scheme relies on the hardness of deciding quadratic residuosity in the group $\mathbb{Z}_N^*$, for Blum integer $N = p \cdot q$. To construct our SKE scheme Σ_{BG} resilient against related key attacks, we additionally have to stipulate that DDH is hard over the subgroup of quadratic residues QR_N. In comparison to Σ_{BHHO} from Section 3.1, which is based on DDH alone, we achieve security against a larger class of KDM functions here (functions of type $a \cdot k \oplus \Delta$). This makes the scheme a direct candidate for Applebaum's optimization of garbled circuits [3], a property that Σ_{BHHO} lacks.

QR assumption. Let N be a Blum integer of bitlength λ. With $\mathbb{Z}_N^*[+1]$ we denote the set of elements in $\mathbb{Z}_N^*$ with Jacobi symbol $+1$ and with $\mathsf{QR}_N := \{x^2 \bmod N : x \in \mathbb{Z}_N^*\}$ the set of Quadratic Residues modulo N. Then we say that the Quadratic Residuosity (QR) assumption holds in $\mathbb{Z}_N^*$ if

$$|\mathsf{Pr}[\mathcal{A}(N,x) = 1 : x \leftarrow \mathbb{Z}_N^*[+1]] - \mathsf{Pr}[\mathcal{A}(N,x) = 1 : x \leftarrow \mathsf{QR}_N]|$$

is negligible for all PPT adversaries $\mathcal{A}$.

The SKE scheme Σ'_{BG}. We define the scheme for messages $M \in \{0,1\}$.

- $\mathsf{Pg}(1^\lambda)$ picks a random Blum integer N of length $\ell(\lambda)$.[4] Then samples quadratic residues $g_1, \ldots, g_\lambda \leftarrow \mathsf{QR}_N$ and returns $\pi := (N, g_1, \ldots, g_\lambda)$.
- $\mathsf{Kg}(\pi)$ returns a random bitstring $k \leftarrow \{0,1\}^\lambda$.
- $\mathsf{E}_k(M)$ picks $r_1, \ldots, r_\lambda \leftarrow [N^2]$, computes $g_0 := \prod_{i\in[\lambda]} (g_i^{r_i})^{-k_i}$ and outputs

$$C := (g_1^{r_1}, \ldots, g_\lambda^{r_\lambda}, (-1)^M \cdot g_0) \in \mathbb{Z}_N^{\lambda+1}$$

- $\mathsf{D}_k(C)$ parses C as $(x_1, \ldots, x_\lambda, y)$. Computes $\tilde{M} := y \cdot \prod_{i\in[\lambda]} x_i^{k_i}$. Returns 0 if $\tilde{M} = 1$, returns 1 if $\tilde{M} = -1$, otherwise returns $\perp$.

The $\mathsf{RKA}[\Phi]$ oracle. The $\mathsf{RKA}[\Phi]$ oracle $\mathcal{F}_{\mathsf{RKA}[\Phi]}$ for Σ'_{BG} works exactly like the $\mathsf{RKA}[\Phi]$ for Σ'_{BHHO} from Section 3.1, i.e., Φ allows for transformations of the secret key under XOR. Analogously to Lemma 2 we have

Lemma 10. *$\mathcal{F}_{\mathsf{RKA}[\Phi]}$ is an $\mathsf{RKA}[\Phi]$ oracle for Σ'_{BG} in the sense of Definition 2.*

The $\mathsf{KDM}[\Psi']$ oracle. Although the schemes Σ'_{BHHO} and Σ'_{BG} look strikingly similar, the latter features security against a larger class of KDM functions. Concretely,

$$\Psi' := \{\psi_{a,i,b} : \{0,1\}^\lambda \to \{0,1\}, k \mapsto ak_i \oplus b : i \in [\lambda], a, b \in \{0,1\}\}$$

Given a function $\psi_{a,i,b}$ and a ciphertext $C = (x_1, \ldots, x_\lambda, y)$, the $\mathsf{KDM}[\Psi']$ oracle $\mathcal{F}_{\mathsf{KDM}[\Psi']}$ for Σ'_{BG} simply returns

$$C' := (x'_1, \ldots, x'_\lambda, y') := (x_1, \ldots, x_{i-1}, (-1)^a \cdot x_i, x_{i+1}, \ldots, x_\lambda, y)$$

We check that this decrypts to $ak_i \oplus b$ if $\mathcal{F}_{\mathsf{KDM}[\Psi']}$ is given an honestly generated ciphertext of b (the constant part of $\psi_{i,b}$), i.e., $y = (-1)^b \cdot \prod_{j\in[\lambda]} {x_j}^{-k_j}$:

$$\mathsf{D}_k(C') = y' \cdot \prod_{j\in[\lambda]} {x'_j}^{k_j} \overset{(*)}{=} y \cdot (-1)^{ak_i} \cdot \prod_{j\in[\lambda]} {x_j}^{k_j} = (-1)^{b+ak_i} \cdot \prod_{j\in[\lambda]} {x_j}^{-k_j} \cdot \prod_{j\in[\lambda]} {x_j}^{k_j} = (-1)^{ak_i \oplus b}$$

$(*)$ since $x'_i = (-1)^a \cdot x_i$ and $x'_j = x_j$ for $j \in [\lambda] \setminus \{i\}$.

Lemma 11. *$\mathcal{F}_{\mathsf{KDM}[\Psi']}$ is a $\mathsf{KDM}[\Psi']$ oracle for Σ'_{BG} in the sense of Definition 3 if QR is hard in the underlying group $\mathbb{Z}_N^*$.*

[4] We use $\ell(\lambda)$ here since the IND-CPA security of Brakerski and Goldwasser's original scheme requires that N is substantially shorter than the number of components/key length λ, e.g., $\ell(\lambda) = \lambda/2$. We refer to [23], Theorem 6.1 for details.

Proof. To show the indistinguishability of $\mathcal{F}_{\mathsf{KDM}[\Psi']}$'s output we use the interactive vector game (IV) from [23], Section 5. In the interactive λ-vector game the experiment picks a Blum integer N, a quadratic residues $g_1, \ldots, g_\lambda \leftarrow \mathsf{QR}_N$ and a bit $b \leftarrow \{0,1\}$ and sends $N, g_1, \ldots, g_\lambda$ to a PPT adversary $\mathcal{A}$ that has to guess b. It then provides $\mathcal{A}$ with an oracle that, given a query $a \in \{0,1\}^\lambda$, returns $((-1)^{a_1} g_1^r, \ldots, (-1)^{a_\lambda} g_\lambda^r)$ if $b = 0$ and $(g_1^r, \ldots, g_\lambda^r)$ if $b = 1$ for fresh randomness r. [23] show that $\mathcal{A}$'s advantage is negligible if the QR assumption holds in $\mathbb{Z}_N^*$.

Let $\mathcal{D}$ be a PPT algorithm to distinguish $\mathcal{F}_{\mathsf{KDM}[\Psi']}(\psi, \mathsf{E}_k(M))$ from $\mathsf{E}_k(\psi(k))$ in the sense of Definition 3. We construct an adversary $\mathcal{S}$ on the interactive 1-vector game that utilizes $\mathcal{D}$: First, $\mathcal{S}$ sets π to the parameters $(N, g_1, \ldots, g_\lambda)$ received from the interactive λ-vector game, samples a key $k \leftarrow \{0,1\}^\lambda$ and then sends π and k to $\mathcal{D}$. For each query $\psi_{a,i,b}$ received from $\mathcal{D}$, $\mathcal{S}$ picks randomness $r_1, \ldots, r_{i-1}, r_{i+1}, \ldots, r_\lambda \leftarrow [N^2]$ and queries the interactive λ-vector game with vector $\hat{a} \in \{0,1\}^\lambda$ where $\hat{a}_i := a$ and $\hat{a}_j := 0$ for $j \neq i$. $\mathcal{S}$ gets a response $(x_1, \ldots, x_\lambda)$ and sets $x'_i := x_i$ and $x'_j := x_j^{r_j}$ for $j \neq r$. It then sends $(x'_1, \ldots, x'_\lambda, (-1)^b \cdot \prod_{j \in [\lambda]} {x'_j}^{-k_j})$ to $\mathcal{D}$. It is easy to check that this equals $\mathcal{F}_{\mathsf{KDM}[\Psi']}(\psi_{a,i,b}, \mathsf{E}_k(b; \hat{r}))$ if the bit picked by the λ-vector game is 0, or $\mathsf{E}_k(\psi(k); \hat{r})$ otherwise (where randomness $\hat{r} := (rr_1, \ldots, r_{i-1}, r, r_{i+1}, \ldots, rr_\lambda)$).

The advantage of $\mathcal{S}$ is the advantage of $\mathcal{D}$ at the same asymptotic time complexity. Thus, if QR holds in $\mathbb{Z}_N^*$, no such adversary $\mathcal{D}$ with non-negligible advantage can exist. □

IND-CPA security.

Lemma 12. *The SKE scheme Σ'_{BG} is IND-CPA secure if QR is hard in the underlying group $\mathbb{Z}_N^*$ and DDH is hard over the subgroup of of quadratic residues QR_N.*

Proof. This proof is completely analogous to the IND-CPA proof for Σ'_{BHHO} (see Lemma 4). We first collapse the randomness to one random exponent per ciphertext. For this we rely on the hardness of DDH over QR_N. Subsequently we utilize the IND-CPA security of Brakerski and Goldwasser's original scheme to conclude the proof. □

The full scheme Σ_{BG}. Analogously to the setting for BHHO (Section 3.1), we can canonically construct the full scheme Σ_{BG} for message space $\{0,1\}^\lambda$ from λ instances of Σ'_{BG} using the same public parameters and the same key. The class of RKA functions remains the same, while the class of KDM functions automatically extends from Ψ' to

$$\Psi := \{\psi_{\mathbf{a},\mathbf{i},M} : \{0,1\}^\lambda \to \{0,1\}^\lambda, k \mapsto (\mathbf{a}_1 k_{\mathbf{i}1} \oplus M_1, \ldots, \mathbf{a}_\lambda k_{\mathbf{i}\lambda}) : \mathbf{a}, M \in \{0,1\}^\lambda, \mathbf{i} \in [\lambda]^\lambda\}$$

Since we can canonically transfer Lemma 10, Lemma 11 and Lemma 12 from Σ'_{BG} to Σ_{BG} we get the final result of this section by Theorem 1.

Theorem 13. *The SKE scheme Σ_{BG} is $\mathsf{RKA\text{-}KDM}[\Phi, \Psi]$ secure (for Φ and Ψ as defined above in this section) if QR is hard in the underlying group $\mathbb{Z}_N^*$ and DDH is hard over the subgroup of quadratic residues QR_N.*

3.4 Barak et al. [6]

Barak et al. (henceforth BHHI) present a technique to construct bounded-KDM-secure public-key encryption schemes from garbled circuits and a framework they call *targeted encryption*. Bounded KDM security means that the class of KDM functions is the set of all functions that can be represented by a garbled circuit of bounded depth L. We refer to this function class as $\Psi_{\mathsf{bnd}(L)}$ from now on. Their work comprises realizations of targeted encryption based on the PKE schemes from BHHO ([22]) and ACPS ([5]). In this section we transfer our notion of $\mathsf{RKA}[\Phi]$ oracles from Section 3 to targeted encryption in the secret key setting. Furthermore, we observe that an instantiation of targeted encryption and a corresponding $\mathsf{RKA}[\Phi]$ oracle gives us a $\mathsf{RKA\text{-}KDM}[\Phi, \Psi_{\mathsf{bnd}(L)}]$ secure secret key encryption scheme. Finally, we present an instantiation from BHHO and note that the targeted encryption version of ACPS also fits our framework.

Targeted encryption. A (symmetric) *targeted encryption scheme* TES consists of a tuple of algorithms $(\mathsf{TPg}, \mathsf{TKg}, \mathsf{TE}, \mathsf{TD})$ such that, given the security parameter λ, $\mathsf{TPg}(1^\lambda)$ generates public parameters π. A secret key k is picked by $k \leftarrow \mathsf{TKg}(\pi)$ where we stipulate $k \in \{0,1\}^\lambda$. We require correctness for the decryption algorithm TD as follows: For every message $M \in \mathcal{M}$ and index $i \in [\lambda]$

$$\mathsf{TD}_k(\mathsf{TE}_{k,i,k_i}(M)) = M$$

This means that an index and a bit can be picked while encrypting M: if the ith key bit equals the picked bit, the ciphertext should decrypt to M. Furthermore, following [6], we define two security properties for targeted encryption schemes:

1. **(Statistical) security against receiver.** For every $k, M, M' \in \{0,1\}^\lambda$ and index $i \in [\lambda]$

   $$\mathsf{TE}_{k,i,1-k_i}(M)) \overset{s}{\approx} \mathsf{TE}_{k,i,1-k_i}(M')$$

   Meaning if the bit picked while encrypting does not equal the ith key bit, the ciphertext doesn't contain any information about M.
2. **Security against outsiders.** For every $M, M' \in \{0,1\}^\lambda$, index $i \in [\lambda]$ and $b \in \{0,1\}$

   $$\mathsf{TE}_{k,i,b}(M) \overset{c}{\approx} \mathsf{TE}_{k,i,b}(M')$$

   meaning no information about the message M is revealed to outsiders who don't know the secret key.

Garbled circuits. We use Yao's garbled circuit construction [34] in the same way as [6] do. We refer to [6] for further details on garbled circuits for this application. This is the transformation of a circuit h with λ input bits and λ pairs of keys $(K_{1,0}, K_{1,1}), \ldots (K_{\lambda,0}, K_{\lambda,1})$ into a garbled circuit G such that the following three properties hold:

1. For input $x \in \{0,1\}^\lambda$ and any choice of 2λ keys, output $h(x)$ can be efficiently decoded without knowing h from G and the λ keys K_{i,x_i} corresponding to x,
2. G and λ keys (corresponding to x) hides everything about h other than the size of h and $h(x)$,
3. G alone computationally hides all information about h other than its size.

The BHHI construction. We now present the targeted encryption construction of [6] in the symmetric setting, keeping notation consistent where possible. Let $(\mathsf{TPg}, \mathsf{TKg}, \mathsf{TE}, \mathsf{TD})$ be a targeted encryption scheme with message space $\mathcal{M} = \{0,1\}^\lambda$ where λ is the security parameter. The construction creates a (symmetric) $\mathsf{RKA\text{-}KDM}[\Phi, \Psi_{\mathsf{bnd}(L)}]$-secure encryption scheme $\Sigma_{\mathsf{BHHI}} = (\mathsf{Pg}, \mathsf{Kg}, \mathsf{E}, \mathsf{D})$ as follows.

- $\mathsf{Pg}(1^\lambda)$ returns the empty bitstring.
- $\mathsf{Kg}(\pi)$ samples and outputs $k \leftarrow \mathsf{TKg}(\pi)$.
- $\mathsf{E}_k(M)$ chooses 2λ random strings $\bar{K} = (K_{i,b})_{(i,b)\in[\lambda]\times\{0,1\}}$ and computes the garbled circuit transformation on $\bar{K}$ and constant function h^M_{const} that outputs M on every input $x \in \{0,1\}^\lambda$, let G be the resulting output. Compute, for every $(i,b) \in [\lambda] \times \{0,1\}$, the value $\tilde{K}_{i,b} = \mathsf{TE}_{k,i,b}(K_{i,b})$ and output $(G, (\tilde{K}_{i,b})_{(i,b)\in[\lambda]\times\{0,1\}})$.
- $\mathsf{D}_k(G, (\tilde{K}_{i,b})_{i,b})$ parses k and computes $K_i = \mathsf{TD}_k(\tilde{K}_{i,k_i})$ for every $i \in \lambda$. Computes and outputs the evaluation of the garbled circuit G on $K_1, \ldots, K_\lambda$.

$\mathsf{RKA}[\Phi]$ oracle. Before we define $\mathsf{RKA}[\Phi]$ oracles we make a quick observation. We cannot hope for a function that, given a ciphertext $C \leftarrow \mathsf{TE}_{k,i,b}(M)$ and $\varphi \in \Phi$, outputs something that is indistinguishable from $\mathsf{TE}_{\varphi(k),i,b}(M)$ for someone who knows $\varphi(k)$ – at least not if Φ is non-trivial. If Φ contains a function that changes any key bit, security against receivers and the existence of an $\mathsf{RKA}[\Phi]$ oracle would be contradictory. Instead, we define the oracle as follows:

Definition 4 ($\mathsf{RKA}[\Phi]$ oracle for targeted encryption)**.** *Let $\mathcal{T} = (\mathsf{TPg}, \mathsf{TKg}, \mathsf{TE}, \mathsf{TD})$ be a (symmetric) targeted encryption scheme. We say that a function $\mathcal{F}_{\mathsf{RKA}[\Phi]}(\varphi, C)$ is an $\mathsf{RKA}[\Phi]$ oracle for $\mathcal{T}$ iff for all PPT adversaries $\mathcal{A}$ that make queries (φ, i, b, M) for $\varphi \in \Phi$, $i \in [\lambda]$, bit $b \in \{0,1\}$, and $M \in \mathcal{M}$*

$$\left| \mathsf{Pr}\left[\mathcal{A}^{\mathcal{F}_{\mathsf{RKA}[\Phi]}(\varphi, \mathsf{TE}_{k,i,b}(M))}(\pi, k) = 1 : \pi \leftarrow \mathsf{Pg}(1^\lambda), k \leftarrow \mathsf{Kg}(\pi)\right] \right.$$
$$\left. - \mathsf{Pr}\left[\mathcal{A}^{\mathsf{TE}_{\varphi(k),i,b\oplus\Delta_i}(M)}(\pi, k) = 1 : \pi \leftarrow \mathsf{Pg}(1^\lambda), k \leftarrow \mathsf{Kg}(\pi)\right] \right|$$

is a negligible function in λ where $\Delta = k \oplus \varphi(k)$, i.e., we have $\Delta_i = 1$ if φ flips the ith bit of k.

Theorem 14. *Let $\mathcal{T} = (\mathsf{TPg}, \mathsf{TKg}, \mathsf{TE}, \mathsf{TD})$ be a (symmetric) targeted encryption scheme and $\mathcal{F}_{\mathsf{RKA}[\Phi]}(\varphi, C)$ be an $\mathsf{RKA}[\Phi]$ oracle for $\mathcal{T}$. Let Ψ denote the class of functions that can be encoded as circuits of bounded depth L. Then the scheme Σ_{BHHI} built from $\mathcal{T}$ is an $\mathsf{RKA\text{-}KDM}[\Phi, \Psi_{\mathsf{bnd}(L)}]$-secure SKE scheme.*

Proof. Our strategy is to first remove the RKA part of queries, and subsequently the proof works analogously to that of Theorem 7 in [6] (because we can deal with the bounded KDM part the same way).

Game 0 Game 0 is the real $\mathsf{RKA\text{-}KDM}[\Phi, \Psi_{\mathsf{bnd}(L)}]$ experiment (as described in Definition 1).

Game 1 In Game 1 we change the way the ciphertexts $\mathsf{TE}_{\varphi(k),i,b}(K_{i,b})$ are created (where $\varphi(k) = k \oplus \Delta$ for some $\Delta \in \{0,1\}^\lambda$). To compute $\mathsf{TE}_{\varphi(k),i,b}(K_{i,b})$ for some i, b, the experiment computes $\mathcal{F}_{\mathsf{RKA}}(\varphi, \mathsf{TE}_{k,i,b\oplus\Delta_i}(K_{i,b}))$. Game 1 is indistinguishable from Game 0 by the $\epsilon_{\mathsf{RKA}}(\lambda)$ indistinguishability of $\mathcal{F}_{\mathsf{RKA}}$. In particular, note that the same selection of keys $K_{i,\varphi(k)}(i \in [\lambda])$ for the garbled circuit can be retrieved by anyone in possession of $\varphi(k)$ from the experiments' output while the keys $K_{i,1-\varphi(k)}$ are lost in both games.

Game 2 In Game 2 we replace the lost keys $K_{i,1-\varphi(k)}$ by 0^λ. This is indistinguishable from Game 1 by the security against receiver of the targeted encryption scheme for k and the fact that the same key material is lost with respect to k and to $\varphi(k)$.

We are now in a position to continue with the proof from the original paper, using the security properties of $\mathcal{T}$ with respect to k. We refer to Section 4.1 of [6] for details. □

Instantiation from BHHO. Our instantiation of targeted encryption is very similar to the scheme Σ_{BHHO} from Section 3.1, and we only adapt the encryption algorithm to suit our targeted encryption requirements. Call $\Sigma'_{\mathsf{TE\text{-}BHHO}}$ the targeted encryption scheme that generates parameters and keys the say way as Σ'_{BHHO} does. For ease of reading we again define the scheme just for messages $M \in \{0,1\}$. It can be extended to message space $\{0,1\}^\lambda$ analogously to Σ'_{BHHO}. We now define the encryption algorithm. $\mathsf{TE}_{k,i,b}(M)$ picks $(r_1, \ldots, r_\lambda) \leftarrow \mathbb{Z}_p^\lambda$, computes $g_0 := \prod_{i\in[\lambda]}(g_i^{r_i})^{-k_i}$ and outputs

$$C := \begin{cases} \left(g_1^{r_1}, \ldots, g_{i-1}^{r_{i-1}}, g_i^{r_i} g^{-M}, g_{i+1}^{r_{i+1}}, \ldots, g_\lambda^{r_\lambda}, g^M \cdot g_0\right) & \text{if } b = 0 \\ \left(g_1^{r_1}, \ldots, g_{i-1}^{r_{i-1}}, g_i^{r_i} g^{M}, \;\; g_{i+1}^{r_{i+1}}, \ldots, g_\lambda^{r_\lambda}, g_0\right) & \text{otherwise } (b = 1) \end{cases}$$

Decryption works as in Σ'_{BHHO}.

Lemma 15. *$\Sigma'_{\mathsf{TE\text{-}BHHO}}$ is a TES if DDH is hard over the underlying group $\mathbb{G}$.*

Proof. We first check the properties of targeted encryption for $\Sigma_{\mathsf{TE\text{-}BHHO}}$.

1. Correctness. Let $C := (x_1, \ldots, x_\lambda, y) \leftarrow \mathsf{TE}_{k,i,k_i}(M)$.
   If $k_i = 0$, decryption computes $y \cdot \prod_{i\in[\lambda]} x_i^{k_i} = g^M \cdot g_0 \left(\prod_{i\in[\lambda]} (g_i^{r_i})^{k_i}\right) = g^M$. This holds since $x_i^0 = (g_i^{r_i} g^{-M})^0 = (g_i^{r_i})^0$.
   If $k_i = 1$, decryption computes $y \cdot \prod_{i\in[\lambda]} x_i^{k_i} = g_0 \left(\prod_{i\in[\lambda]} (g_i^{r_i})^{k_i}\right) g^M = g^M$.
   Hence we have $\mathsf{TD}_k(\mathsf{TE}_{k,i,k_i}(M)) = M$.
2. (Statistical) security against receiver. Let $C := (x_1, \ldots, x_\lambda, y) \leftarrow \mathsf{TE}_{k,i,1-k_i}(M)$ and $\alpha := \log_{g_i}(g)$. We distinguish two cases:
   (a) $k_i = 0$: We have $x_i = g_i^{r_i} g^M$. For $r_i' := r_i + \alpha(M - M')$ we set $x_i' := g_i^{r_i'} g^{M'}$ and $y' := y$.
   (b) $k_i = 1$: We have $x_i = g_i^{r_i} g^{-M}$ and $y = g^M \cdot g_0$. For $r_i' := r_i - \alpha(M - M')$ we set $x_i' := g_i^{r_i'} g^{-M'}$ and observe $y = g^M \cdot g_0 = g^M g^{-(M-M')} g^{(M-M')} g_0 = g^{M'} g_i^{\alpha(M-M')} g_0 = g^{M'} g_0' =: y'$ where g_0' is computed like g_0 but with $g_i^{-r_i'}$ instead of $g_i^{r_i}$.
   In both cases $(x_1, \ldots, x_{i-1}, x_i', x_{i+1}, \ldots x_\lambda, y')$ is the output of $\mathsf{TE}_{k,i,1-k_i}(M')$ under randomness $(r_1, \ldots, r_{i-1}, r_i', r_{i+1}, \ldots r_\lambda)$ which differs only by an offset in the ith component from the randomness for C. Hence the distributions are perfectly indistinguishable.
3. Security against outsiders. First, note that security against outsiders is equivalent to distinguishing encryptions of a message M to encryptions of 0 (a chance of distinguishing then exists only for $M = 1$). Security against outsiders follows from the $\mathsf{RKA\text{-}KDM}[\Phi, \Psi]$ security of the original scheme from Section 3.1 and the indistinguishability of the corresponding RKA and KDM oracles.

□

The $\mathsf{RKA}[\Phi]$ oracle. We construct the $\mathsf{RKA}[\Phi]$ oracle $\mathcal{F}_{\mathsf{RKA}[\Phi]}$ for $\Sigma'_{\mathsf{TE\text{-}BHHO}}$ exactly like that for Σ'_{BHHO} in Section 3.1. I.e., the class of RKA functions is

$$\Phi := \{\varphi_\Delta : \{0,1\}^\lambda \to \{0,1\}^\lambda, k \mapsto k \oplus \Delta : \Delta \in \{0,1\}^\lambda\}$$

Let $C := (x_1, \ldots, x_\lambda, y) \leftarrow \mathsf{TE}_{k,i,b}(M)$. If the jth key bit is flipped, the oracle multiplies x_j with y and inverts x_j. For the sake of readability we assume that only one bit is flipped (the general case with multiple bits being flipped follows canonically). For $i \neq j$ the output is indistinguishable from $\mathsf{TE}_{k',i,b}(M)$ (where k' is k with the jth bit flipped) following the reasoning from Lemma 2. For $i = j$ we distinguish two cases:

1. $b = 0$: Then $x_i' := x_i^{-1} = g_i^{-r_i} g^M$ and $y' := x_i \cdot y = g_i^{r_i} g^{-M} \cdot g^M g_0 = g_i^{r_i} g_0 = \left(g_i^{-r_i}\right)^{-1} g_0$. Thus the output is now indistinguishable from a ciphertext for $b = 1$ (where $r_i' := -r_i$).
2. $b = 1$: Then $x_i' := x_i^{-1} = g_i^{-r_i} g^{-M}$ and $y' := x_i \cdot y = g_i^{r_i} g^M \cdot g_0 = g^M \left(g_i^{-r_i}\right)^{-1} g_0$. Here the output is indistinguishable from a ciphertext for $b = 0$ (again $r_i' := -r_i$).

Lemma 16. *$\mathcal{F}_{\mathsf{RKA}[\Phi]}$ is an $\mathsf{RKA}[\Phi]$ oracle for targeted encryption (Definition 4)*

As sketched above, the proof of indistinguishability works in an analogous manner to that of Lemma 2.

Instantiation from ACPS. We note that the authors of [6] also present an instantiation of targeted encryption from the ACPS scheme [5]. Instead of the original ACPS scheme, we can also interpret our own secret-key version of the ACPS scheme from Section 3.2 as a targeted encryption scheme (with RKA oracle). (This is done completely analogously to the case of our interpretation of the BHHO scheme as a targeted encryption scheme above.) We thus obtain a targeted encryption scheme from the LWE assumption.

4 Malkin et al. [31]

We now turn our attention to the work of Malkin, Teranishi and Yung (henceforth MTY) [31], who provide an efficient PKE scheme which is KDM secure with respect to functions computable by polynomial-size modular arithmetic circuits (MACs). We present a symmetric version of their scheme that is $\mathsf{RKA\text{-}KDM}[\Phi, \Psi]$ with respect to the RKA function class of modular addition and affine KDM functions.

DCR assumption. Let N be a RSA modulus of length λ, and let $\mathsf{CR}_{N^2} = \{u^N \bmod N^2 | u \in \mathbb{Z}^*_{N^2}\}$ be the set of Nth Residues modulo N^2. We say that the *Decisional Composite Residuosity (DCR) assumption* holds in $\mathbb{Z}^*_{N^2}$ if

$$\left|\mathsf{Pr}[\mathcal{A}(N, x) = 1 : x \leftarrow \mathbb{Z}^*_{N^2}] - \mathsf{Pr}[\mathcal{A}(N, x) = 1 : x \leftarrow \mathsf{CR}_{N^2}]\right|$$

is negligible for all PPT adversaries $\mathcal{A}$.

We consider MTY's so-called Cascaded Paillier Elgamal scheme in the case where $s = 2$ (the exponent of N) and $d = 1$ (the maximum degree of the polynomials used as KDM queries) to reflect affine functions. In this case the scheme for messages $M \in \mathbb{Z}_N$ works as follows:

- $\mathsf{Pg}(1^\lambda)$ generates N as the product of two safe primes with $\lfloor \lambda/2 \rfloor$ bit lengths. Randomly chooses $g \leftarrow \mathsf{CR}[N^2]$ with full order $\varphi_{\mathsf{E}}(N)/4$ and and outputs $\pi := (N, g)$. Here φ_{E} denotes Euler's Phi Function.
- $\mathsf{Kg}(\pi)$ returns $k \leftarrow [\lfloor N/4 \rfloor]$.
- $\mathsf{E}_k(M)$ randomly chooses $r \leftarrow [\lfloor N/4 \rfloor]$, computes $x := g^{-r} \bmod N^2$ and $y := (1 + N)^M g^{rk} \bmod N^2$ and outputs $C := (x, y)$.
- $\mathsf{D}_k(C)$ parse C as (x, y), computes $(1 + N)^M = x^k y \bmod N^2$ and recovers M using the efficient bijection described in original paper.

The $\mathsf{RKA}[\Phi]$ oracle. For the concrete class of RKA functions $\Phi := \{\varphi_\Delta(k) := k + \Delta \bmod \varphi_{\mathsf{E}}(N)/4 : \Delta \in \mathbb{Z}\}$ we find an $\mathsf{RKA}[\Phi]$ oracle $\mathcal{F}_{\mathsf{RKA}[\Phi]}$ for the MTY scheme as follows: $\mathcal{F}_{\mathsf{RKA}[\Phi]}(\varphi_\Delta, C)$ parses C as (x, y) and computes $(x, y \cdot x^{-\Delta} \bmod N^2)$.

Lemma 17. *$\mathcal{F}_{\mathsf{RKA}[\Phi]}$ is an $\mathsf{RKA}[\Phi]$ oracle in the sense of Definition 2.*

Proof. Observe that $(x, y \cdot x^{-\Delta}) = (g^{-r}, (1 + N)^M g^{rk} g^{r\Delta}) = (g^{-r}, (1 + N)^M g^{r(k+\Delta)})$. Hence, given a valid encryption of M, the output of the oracle is the encryption of M under key $k + \Delta \bmod \varphi_{\mathsf{E}}(N)/4$ and randomness r. □

The KDM and IND-CPA properties of our variant of the MTY scheme follow directly from the analysis in [31]; for completeness, we provide formal proofs in our notation.

The $\mathsf{KDM}[\Psi]$ oracle. The class of KDM functions here is affine functions modulo N, namely $\Psi := \{\psi_{a,M}(k) := ak + M \bmod N : a, M \in \mathbb{Z}_N\}$. We find the following $\mathsf{KDM}[\Psi]$ oracle $\mathcal{F}_{\mathsf{KDM}[\Psi]}$ for the scheme: Given a function $\psi_{a,M}$ and $C = (x, y)$, a (valid) ciphertext of M, it outputs

$$(x \cdot (1 + N)^a, y) =: C' = (x', y').$$

We show that C' decrypts to $ak + M \bmod N$ under key k:

$$\mathsf{D}_k(C') = (x')^k \cdot y' = (1 + N)^{ak} \cdot (g^{-r})^k \cdot (1 + N)^M g^{rk} = (1 + N)^{ak+M} \bmod N^2.$$

Lemma 18. *$\mathcal{F}_{\mathsf{KDM}[\Psi]}$ is an indistinguishable $\mathsf{KDM}[\Psi]$ oracle in the sense of Definition 3.*

Proof. We use the first interactive vector game IV_1 from [31] for this proof. The simulator picks a key $k \leftarrow [\lfloor N/4 \rfloor]$. For each query $\psi_{a,M}$ by the adversary, the simulator sends $-a$ to IV_1 and receives the response $u := g^r(1+N)^{-ab}$ where $b \in \{0,1\}$ and $g \in \mathsf{CR}[N^2]$ are picked uniformly by IV_1 for all queries and r is some uniform randomness that's fresh for each query. The simulator sends the ciphertext $C := (u^{-1}, u^k \cdot (1+N)^{ak+M})$ to the adversary. For $b = 0$ this is $\left(g^{-r}, g^{rk}(1+N)^{ak+M}\right)$ which is a response to the KDM query $\psi_{a,M}$ in the real game. For $b = 1$ the output is $\left(g^{-r}(1+N)^a, g^{rk}(1+N)^M\right)$ which is the output in the oracle-based game. By Lemma 1 of [31], the advantage of any adversary guessing b in IV_1 is negligible under the DCR assumption.

Note that in IV_1 in the original paper [31], g is picked from $\{t^{4N} \bmod N^2 | t \in \mathbb{Z}_{N^2}\}$ rather than from $\mathsf{CR}[N^2]$, which could lead to a bad event if g does not have the correct order. We observe that this only occurs with negligible probability. This concludes our proof. □

IND-CPA security.

Lemma 19. *The SKE scheme Σ_{MTY} is IND-CPA secure if DCR is hard in the underlying group $\mathbb{Z}^*_{N^2}$.*

Proof. We use the second interactive vector game IV_2 from [31] to prove the scheme IND-CPA secure. When the adversary queries an encryption of M, the simulator sends $(0, M)$ to IV_2. It receives the response $(u, v) := (g^r, (1+N)^{bM}h^r)$ where $b \in \{0,1\}$ and $g, h \in \mathsf{CR}[N^2]$ are picked uniformly by IV_2 for all queries and r is some uniform randomness that is fresh for each query. Since g is of full order $\varphi_{\mathsf{E}}(N)/4$ there is some $k \in [\lfloor N/4 \rfloor]$ such that $g^k = h$. This is the key implicitly chosen by IV_2. The simulator sends the ciphertext $C := (u^{-1}, v)$ to the adversary. This is a legitimate ciphertext of bM under k and is hence the response of the real IND-CPA experiment for $b = 0$ and $b = 1$ respectively. By Lemma 1, [31], the advantage of any adversary guessing b in IV_2 is negligible under the DCR assumption. This concludes our proof. Again, we note that in the original IV_2, g is picked from $\{t^{4N} \bmod N^2 | t \in \mathbb{Z}_{N^2}\}$ rather than from $\mathsf{CR}[N^2]$, which could lead to a bad event if g does not have the correct order. We observe that this only occurs with negligible probability. □

Finally, by Lemma 17, Lemma 18, Lemma 19 and Theorem 1, we obtain

Theorem 20. *The scheme Σ_{MTY} is $\mathsf{RKA\text{-}KDM}[\Phi, \Psi]$ secure (for Φ and Ψ as defined above in this section) if the DCR assumption holds in $\mathbb{Z}^*_{N^2}$.*

Acknowledgements. The authors would like to thank Martijn Stam for useful discussions and Rafael Dowsley for kindling our interest in the topic.

References

[1] Pedro Adão, Gergei Bana, Jonathan Herzog, and Andre Scedrov. Soundness of Formal Encryption in the Presence of Key-Cycles. In *ESORICS*, pages 374–396, 2005.

[2] Adi Akavia, Shafi Goldwasser, and Vinod Vaikuntanathan. Simultaneous Hardcore Bits and Cryptography against Memory Attacks. In *TCC*, pages 474–495, 2009.

[3] Benny Applebaum. Garbling XOR gates "For Free" in the Standard Model. In *TCC*, pages 162–181, 2013.

[4] Benny Applebaum. Key-Dependent Message Security: Generic Amplification and completeness. In *EUROCRYPT*, pages 527–546, 2011.

[5] Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. Fast Cryptographic Primitives and Circular-Secure Encryption based on Hard Learning Problems. In *CRYPTO*, pages 595–618, 2009.

[6] Boaz Barak, Iftach Haitner, Dennis Hofheinz, and Yuval Ishai. Bounded Key-Dependent Message Security. In *EUROCRYPT*, pages 423–444, 2010.

[7] Mihir Bellare and David Cash. Pseudorandom Functions and Permutations Provably Secure against Related-Key Attacks. In *CRYPTO*, pages 666–684, 2010.

[8] Mihir Bellare and Sriram Keelveedhi. Authenticated and Misuse-Resistant Encryption of Key-Dependent Data. In *CRYPTO*, pages 610–629, 2011.

[9] Mihir Bellare and Tadayoshi Kohno. A Theoretical Treatment of Related-Key Attacks: RKA-PRPs, RKA-PRFs, and Applications. In *EUROCRYPT*, pages 491–506, 2003.

[10] Mihir Bellare, Zvika Brakerski, Moni Naor, Thomas Ristenpart, Gil Segev, Hovav Shacham, and Scott Yilek. Hedged Public-Key Encryption: How to Protect against Bad Randomness. In *ASIACRYPT*, pages 232–249, 2009.

[11] Mihir Bellare, Dennis Hofheinz, and Scott Yilek. Possibility and Impossibility Results for Encryption and Commitment Secure under Selective Opening. In *EUROCRYPT*, pages 1–35, 2009.

[12] Mihir Bellare, David Cash, and Sriram Keelveedhi. Ciphers that Securely Encipher their own Keys. In *ACM Conference on Computer and Communications Security*, pages 423–432, 2011.

[13] Mihir Bellare, David Cash, and Rachel Miller. Cryptography Secure against Related-Key Attacks and Tampering. In *ASIACRYPT*, pages 486–503, 2011.

[14] Eli Biham. New types of Cryptoanalytic Attacks using Related Keys. In *EUROCRYPT*, pages 398–409, 1993.

[15] Eli Biham, Orr Dunkelman, and Nathan Keller. A Related-Key Rectangle Attack on the Full KASUMI. In *ASIACRYPT*, pages 443–461, 2005.

[16] Eli Biham, Orr Dunkelman, and Nathan Keller. Related-Key Impossible Differential Attacks on 8-Round AES-192. In *CT-RSA*, pages 21–33, 2006.

[17] Eli Biham, Orr Dunkelman, and Nathan Keller. A Simple Related-Key Attack on the Full SHACAL-1. In *CT-RSA*, pages 20–30, 2007.

[18] Alex Biryukov and Dmitry Khovratovich. Related-Key Cryptanalysis of the Full AES-192 and AES-256. In *ASIACRYPT*, pages 1–18, 2009.

[19] Alex Biryukov, Dmitry Khovratovich, and Ivica Nikolic. Distinguisher and Related-Key Attack on the Full AES-256. In *CRYPTO*, pages 231–249, 2009.

[20] Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, and Adi Shamir. Key Recovery Attacks of Practical Complexity on AES-256 Variants with up to 10 Rounds. In *EUROCRYPT*, pages 299–319, 2010.

[21] John Black, Phillip Rogaway, and Thomas Shrimpton. Encryption-Scheme Security in the Presence of Key-Dependent Messages. In *Selected Areas in Cryptography*, pages 62–75, 2002.

[22] Dan Boneh, Shai Halevi, Michael Hamburg, and Rafail Ostrovsky. Circular-secure encryption from Decision Diffie-Hellman. In *CRYPTO*, pages 108–125, 2008.

[23] Zvika Brakerski and Shafi Goldwasser. Circular and Leakage Resilient Public-Key Encryption under Subgroup Indistinguishability - (or: Quadratic Residuosity strikes back). In *CRYPTO*, pages 1–20, 2010.

[24] Zvika Brakerski, Shafi Goldwasser, and Yael Tauman Kalai. Black-Box Circular-Secure Encryption beyond Affine Functions. In *TCC*, pages 201–218, 2011.

[25] Jan Camenisch, Nishanth Chandran, and Victor Shoup. A Public Key Encryption Scheme Secure against Key Dependent Chosen Plaintext and Adaptive Chosen ciphertext Attacks. In *EUROCRYPT*, pages 351–368, 2009.

[26] Stefan Dziembowski and Krzysztof Pietrzak. Leakage-Resilient Cryptography. In *FOCS*, pages 293–302, 2008.

[27] Shafi Goldwasser and Silvio Micali. Probabilistic Encryption. *J. Comput. Syst. Sci.*, 28(2): 270–299, 1984.

[28] Shai Halevi and Hugo Krawczyk. Security under Key-Dependent Inputs. In *ACM Conference on Computer and Communications Security*, pages 466–475, 2007.

[29] Dennis Hofheinz. Circular Chosen-Ciphertext Security with Compact Ciphertexts. In *EUROCRYPT*, pages 520–536, 2013.

[30] Dennis Hofheinz and Dominique Unruh. Towards Key-Dependent Message Security in the Standard Model. In *EUROCRYPT*, pages 108–126, 2008.

[31] Tal Malkin, Isamu Teranishi, and Moti Yung. Efficient Circuit-Size Independent Public Key Encryption with KDM Security. In *EUROCRYPT*, pages 507–526, 2011.

[32] Silvio Micali and Leonid Reyzin. Physically Observable Cryptography. In *TCC*, pages 278–296, 2004.

[33] Hoeteck Wee. Public Key Encryption against Related Key Attacks. In *Public Key Cryptography*, pages 262–279, 2012.

[34] Andrew Chi-Chih Yao. How to Generate and Exchange Secrets. In *FOCS*, pages 162–167, 1986.