Encryption schemes secure under related-key and key-dependent message attacks

Florian Böhl[1⋆], Gareth T. Davies[2⋆⋆], and Dennis Hofheinz[1⋆⋆⋆]

[1] Karlsruhe Institute of Technology (KIT)
[2] University of Bristol

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. RKA-KDM security for our schemes holds w.r.t. affine functions (over the respective mathematical domain).

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.

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,

⋆ Supported by MWK grant "MoSeS".
⋆⋆ Work partially conducted while visiting KIT.
⋆⋆⋆ Supported by DFG grant GZ HO 4534/2-1.

in certain applications, ciphertext indistinguishability is not sufficient. For instance, in harddisk encryption, encryptions of the secret key itself naturally occur (see [25]). Security in the presence of such key-dependent messages (KDM security [23]) is not implied by IND-CPA or IND-CCA security [23, 1]. There are numerous other specialized notions of encryption scheme security, such as security under related-key attacks (RKAs [7]), leakage-resilience [35, 29], 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 [4] (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 [4] 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 [30][3]), 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 [23]), 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. [23, 31, 33, 25, 5, 28, 6, 26, 27, 34, 8, 12, 3, 32]. However, most of these works follow the design principle of Boneh et al. [25] (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

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

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. [16, 17, 18, 19, 21, 20, 22]. There are also a number of constructions of RKA secure schemes, e.g. [7, 13, 36, 4]. 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 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 [4] (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) [4], and decisional composite residuosity (DCR) assumptions. Our constructions support affine KDM and RKA functions in the "natural domain" of the respective secret keys. Furthermore, with the exception of the DCR-based scheme, all of our schemes can be directly used in the application of Applebaum [4]. Additionally, they fit the construction of Bellare et al. [14], and thus can be extended from projection-KDM security to bounded-KDM security while maintaining the same level of RKA security.

Our approach. Based on an informal remark of Applebaum [4, 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

[4] Similar to Hofheinz [32], we have to use the DDH assumption in the group of quadratic residues modulo N.

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 [25, 5, 6, 26, 34]. 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.

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 [25]). 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 [25], all r_i are identical.)

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 [4].) 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 [25].[5]

Our other constructions proceed similarly, starting from the schemes of Applebaum et al. [5], Brakerski and Goldwasser [26], and Malkin et al. [34]. The latter is only contained in our full version [24].

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,

[5] We note that our technical change to the scheme from [25] – namely, using *different* r_i – can be proven to be not crucial to its security (see Lemma 7). Instead, choosing different r_i simplifies expressing the scheme in our framework, and in particular separating the KDM, RKA, and IND-CPA properties.

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 $X \stackrel{c}{\approx} Y$) 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 $X \stackrel{s}{\approx} Y$) 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.

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. Here, $\mathcal{A}^{\mathcal{F}_{\mathsf{RKA}[\Phi]}(\varphi, \mathsf{E}_k(\cdot))}$ denote the interaction of $\mathcal{A}$ with an oracle that, upon input M, outputs $\mathcal{F}_{\mathsf{RKA}[\Phi]}(\varphi, \mathsf{E}_k(M))$.

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, i.e., $\psi(0)$)*

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

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 4. *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. [25]

The PKE scheme of Boneh et al. [25] 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 $\boldsymbol{\Sigma'_{\mathsf{BHHO}}}$. 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 $g_1, \ldots, g_\lambda \leftarrow \mathbb{G}\backslash\{1\}$ 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 5. *$\mathcal{F}_{\mathsf{RKA}[\Phi]}$ 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

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

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

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

We check that this ciphertext decrypts to $k_i \oplus b$:

$$y \cdot \prod_{j\in[\lambda]} {x'_j}^{k_j} \overset{(*)}{=} y \cdot \left(\prod_{j\in[\lambda]} {x_j}^{k_j}\right) \cdot g^{(-1)^b \cdot k_i} = g^b \cdot \left(\prod_{j\in[\lambda]} {x_j}^{-k_j} \cdot {x_j}^{k_j}\right) \cdot g^{(-1)^b \cdot k_i} = g^{k_i \oplus b}$$

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

Lemma 6. *$\mathcal{F}_{\mathsf{KDM}[\Psi']}$ is a $\mathsf{KDM}[\Psi']$ oracle in the sense of Definition 3.*

Proof. We show that the distributions of $\mathcal{F}_{\mathsf{KDM}[\Psi']}(\psi_{i,b}, \mathsf{E}_k(b))$ and $\mathsf{E}_k(\psi_{i,b}(k))$ 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., $x'_i = g^{r_i + (-1)^b \cdot \alpha}$. Furthermore we have $y = g^b \cdot \prod_{j\in[\lambda]} {x_j}^{-k_j} = g^b \cdot \prod_{j\in[\lambda]} {x_j}^{-k_j} g^{-(-1)^b \cdot k_i} g^{(-1)^b \cdot k_i} = g^{b+(-1)^b} \cdot \prod_{j\in[\lambda]} {x'_j}^{-k_j}$. Hence the output of the oracle looks like a normal encryption of $k_i \oplus b$ where $r_i + (-1)^b \cdot \alpha$ was used as randomness in the ith component.

Lemma 7. *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 [25] 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

$$\Psi := \{\psi_{\mathbf{i},\Delta} : \{0,1\}^\lambda \to \{0,1\}^\lambda, k \mapsto (k_{\mathbf{i}_1} \oplus \Delta_1, \ldots, k_{\mathbf{i}_\lambda} \oplus \Delta_\lambda) : \mathbf{i} \in [\lambda]^\lambda, \Delta \in \{0,1\}^\lambda\}$$

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 5 and Lemma 5 carry over to Σ_{BHHO}. Analogously for the IND-CPA security of Σ_{BHHO}. Finally, by Theorem 4, we get

Theorem 8. *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 9. *$\mathcal{F}_{\mathsf{RKA}[\Phi]}$ is an $\mathsf{RKA}[\Phi]$ oracle in the sense of Definition 2.*

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

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

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

$$C' := \left(\mathbf{y} + \left((-1)^b p\right)\mathbf{e}_i, z\right) \qquad \text{for the } i\text{-th unit vector } \mathbf{e}_i.$$

We check that this ciphertext decrypts to $k_i \oplus b$:

$$\mathsf{D}_k(C') = \left\lceil \left(\left\langle \mathbf{s}; \mathbf{y} + \left((-1)^b p\right)\mathbf{e}_i \right\rangle + z\right)/p \right\rfloor_p = \left\lceil \left(\langle \mathbf{s}; \mathbf{y}\rangle + \left((-1)^b p\right)\mathbf{s}_i + z\right)/p \right\rfloor_p$$
$$= \left\lceil \left(\mathbf{s}^T\mathbf{A}\mathbf{r} + \left((-1)^b p\right)\mathbf{s}_i + z\right)/p \right\rfloor_p = \left\lceil \left(\left((-1)^b p\right)\mathbf{s}_i - \langle \mathbf{x}; \mathbf{r}\rangle + pb\right)/p \right\rfloor_p, = \mathbf{s}_i \oplus b.$$

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

Lemma 10. *$\mathcal{F}_{\mathsf{KDM}[\Psi']}$ is a $\mathsf{KDM}[\Psi']$ oracle in the sense of Definition 3.*

Lemma 11. *The SKE scheme Σ'_{ACPS} is IND-CPA secure if the LWE assumption holds for the respective parameters.*

A sketch of the proof is contained in the full version of this paper [24].

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 9, Lemma 10 and Lemma 11 from Σ'_{ACPS} to Σ_{ACPS} and by Theorem 4, we get

Theorem 12. *The SKE scheme Σ_{ACPS} is RKA-$\mathsf{KDM}[\Phi, \Psi]$ secure (for Φ as defined above in this section and Ψ from the full BHHO scheme) if the LWE assumption holds for the respective parameters.*

3.3 Brakerski-Goldwasser [26]

In this section we consider the encryption scheme of Brakerski and Goldwasser [26], 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. We achieve security against the same class of KDM functions as for Σ_{BHHO} from Section 3.1.

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 $\ell(\lambda)$.[6] 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 5 we have

Lemma 13. *$\mathcal{F}_{\mathsf{RKA}[\Phi]}$ is an $\mathsf{RKA}[\Phi]$ oracle for Σ'_{BG} in the sense of Definition 2.*

The $\mathsf{KDM}[\Psi']$ oracle. Analogously to Σ'_{BHHO} we define

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

Given a function $\psi_{i,b}$ 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

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

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

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

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

[6] 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 [26], Theorem 6.1 for details.

Lemma 14. *$\mathcal{F}_{\mathsf{KDM}[\Psi']}$ is a $\mathsf{KDM}[\Psi']$ oracle for Σ'_{BG} in the sense of Definition 3 if QR is hard in the underlying group $\mathbb{Z}_N^*$.*

Proof. To show the indistinguishability of $\mathcal{F}_{\mathsf{KDM}[\Psi']}$'s output we use the interactive vector game (IV) from [26], 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 $\mathbf{a} \in \{0,1\}^\lambda$, returns $((-1)^{\mathbf{a}_1} g_1^r, \ldots, (-1)^{\mathbf{a}_\lambda} g_\lambda^r)$ if $b = 0$ and $(g_1^r, \ldots, g_\lambda^r)$ if $b = 1$ for fresh randomness r. [26] 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 $\psi_{i,b}$ 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 $\mathbf{a} \in \{0,1\}^\lambda$ where $\mathbf{a}_i := 1$ and $\mathbf{a}_j := 0$ 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 $\mathcal{F}_{\mathsf{KDM}[\Psi']}(\psi_{i,b}, \mathsf{E}_k(b; \hat{r}))$ 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.

Lemma 15. *The SKE scheme Σ'_{BG} is IND-CPA secure if QR is hard over the group $\mathbb{Z}_N^*$ and DDH is hard over the subgroup of quadratic residues QR_N.*

Proof. This proof is completely analogous to the IND-CPA proof for Σ'_{BHHO} (see Lemma 7). 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

$$\Psi := \{\psi_{\mathbf{i},M} : \{0,1\}^\lambda \to \{0,1\}^\lambda, k \mapsto (k_{\mathbf{i}_1} \oplus \Delta_1, \ldots, k_{\mathbf{i}_\lambda} \oplus \Delta_\lambda) : \mathbf{i} \in [\lambda]^\lambda, \Delta \in \{0,1\}^\lambda\}$$

Since we can canonically transfer Lemma 13, Lemma 14 and Lemma 15 from Σ'_{BG} to Σ_{BG} we get the final result of this section by Theorem 4.

Theorem 16. *The SKE scheme Σ_{BG} is RKA-$\mathsf{KDM}[\Phi, \Psi]$ 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 Bellare et al. [14]

Since Applebaum's work on KDM amplification [3], it is known that projection-KDM security implies bounded-KDM security. Projection-KDM security allows for KDM functions where each output bit depends only on one input bit (key bit). Bounded-KDM security means that the class of KDM functions is the set of all functions that can be represented by a circuit of bounded size L. We refer to this function class as $\Psi_{\mathsf{bnd}(L)}$ from now on. To our knowledge, currently the most efficient way to construct a bounded-KDM secure scheme from a projection-KDM secure one is the approach of Bellare, Hoang, and Rogaway [14] (henceforth BHR). In this section we observe that their construction also maintains RKA security in our sense. Thus, we can plug all of our projection-KDM secure schemes (i.e., Σ_{BG}, Σ_{ACPS} and Σ_{BHHO}) into their framework to get RKA-bounded-KDM secure schemes. Obviously, this result holds for any projection-KDM secure scheme that is RKA secure (with a suitable oracle in our sense).

(Projective) garbling schemes. What follows is a quick introduction to garbling schemes established by [14]. A *garbling scheme* is a tuple of algorithms $(\mathsf{GC}_{\mathsf{garble}}, \mathsf{GC}_{\mathsf{encode}}, \mathsf{GC}_{\mathsf{decode}}, \mathsf{GC}_{\mathsf{eval}})$.[7] The algorithm $\mathsf{GC}_{\mathsf{garble}}$ is probabilistic while the remaining algorithms are deterministic. Given an encoding of the security parameter and a function f, $\mathsf{GC}_{\mathsf{garble}}(1^\lambda, f)$ outputs the description of a garbled circuit (F, e, d). Here, F is a function mapping garbled inputs to garbled outputs. E.g., F could be a circuit in terms of gates and wires together with a garbled table for each gate. The outputs e and d contain information to encode and decode the input and output of F respectively. We say that a garbling scheme is *correct* if $\mathsf{GC}_{\mathsf{decode}}(d, \mathsf{GC}_{\mathsf{eval}}(F, \mathsf{GC}_{\mathsf{encode}}(M, e))) = f(M)$ for all functions f (from a certain class), inputs $M \in \{0,1\}^\lambda$ and descriptions $(F, e, d) \leftarrow \mathsf{GC}_{\mathsf{garble}}(1^\lambda, f)$ of garbled circuits for f.

For our application we need so-called *projective* garbling schemes. Basically, a garbling scheme is *projective* if for all $\mathbf{x} := \mathsf{GC}_{\mathsf{encode}}(e, M)$ and $\mathbf{x}' := \mathsf{GC}_{\mathsf{encode}}(e, M')$, we have $|\mathbf{x}_i| = |\mathbf{x}'_i|$ for $i \in [\lambda]$ and $\mathbf{x}_i = \mathbf{x}'_i$ for $i \in [\lambda]$ with $M_i = M'_i$ (see [15] for a rigorous definition). One well-known way to construct a projective garbling scheme is to assign a pair of keys to each wire corresponding to low and high voltage (0/1) respectively. Then e is a tuple of pairs of keys and $\mathsf{GC}_{\mathsf{encode}}(M, e)$ picks the keys from e corresponding to the bits of M.

Furthermore, we say that a garbling scheme is *privacy preserving* if for any two (adversarially chosen) functions f_0, f_1 with the same circuit size and inputs x_0, x_1 of same length with $f_0(x_0) = f_1(x_1)$, no adversary can distinguish $(F_0, \mathsf{GC}_{\mathsf{encode}}(e_0, x_0), d_0)$ from $(F_1, \mathsf{GC}_{\mathsf{encode}}(e_1, x_1), d_1)$ (where $(F_b, e_b, d_b) \leftarrow \mathsf{GC}_{\mathsf{garble}}(1^\lambda, f_b), b \in \{0,1\}$). We refer to [15] for a more detailed definition.

The construction of BHR. The construction creates a symmetric $\mathsf{KDM}[\Psi_{\mathsf{bnd}(L)}]$-secure encryption scheme $\Sigma_{\mathsf{BHR}} = (\mathsf{Pg}, \mathsf{Kg}, \mathsf{E}, \mathsf{D})$ from any projection-KDM-

[7] For simplicity we omit the additional evaluation function from [14] and restrict to inputs of length λ here.

secure encryption scheme $\Sigma' = (\mathsf{Pg}', \mathsf{Kg}', \mathsf{E}', \mathsf{D}')$ and any privacy preserving projective garbling scheme $(\mathsf{GC}_{\mathsf{garble}}, \mathsf{GC}_{\mathsf{encode}}, \mathsf{GC}_{\mathsf{decode}}, \mathsf{GC}_{\mathsf{eval}})$ as follows.

- $\mathsf{Pg}(1^\lambda)$ returns $\mathsf{Pg}'(1^\lambda)$.
- $\mathsf{Kg}(\pi)$ returns $\mathsf{Kg}'(\pi)$.
- $\mathsf{E}_k(M)$ first generates a garbled circuit for the identity function ID_λ on bit-strings of length λ: $(F, e, d) \leftarrow \mathsf{GC}_{\mathsf{garble}}(1^\lambda, \mathsf{ID}_\lambda)$. It then encodes the message $\mathbf{x} := \mathsf{GC}_{\mathsf{encode}}(e, M)$ (w.l.o.g. $\mathbf{x} \in \{0,1\}^{\lambda \times \lambda}$). Finally, it outputs the ciphertext $C := (F, d, \mathsf{E}'_k(\mathbf{x}_i))$.
- $\mathsf{D}_k((F, d, (\mathbf{c}_i)_{i\in[\lambda]}))$ first decrypts the keys for the input wires $\mathbf{x}_i := \mathsf{D}'_k(\mathbf{c}_i)$ and then evaluates the circuit to compute and output the message $M := \mathsf{GC}_{\mathsf{decode}}(d, \mathsf{GC}_{\mathsf{eval}}(F, \mathbf{x}))$.

An RKA[Φ] oracle for Σ_{BHR}. Given an $\mathsf{RKA}[\Phi]$ oracle $\mathcal{F}'_{\mathsf{RKA}[\Phi]}$ for Σ', we can construct an $\mathsf{RKA}[\Phi]$ oracle $\mathcal{F}_{\mathsf{RKA}[\Phi]}$ for Σ_{BHR} (note that we maintain the class of RKA functions). Let $C = (F, d, (\mathbf{c}_i)_{i\in[\lambda]})$ be an honestly generated ciphertext and $\varphi \in \Phi$ be an RKA function. We define $\mathcal{F}_{\mathsf{RKA}[\Phi]}(C) := (F, d, (\mathcal{F}'_{\mathsf{RKA}[\Phi]}(\mathbf{c}_i))_{i\in[\lambda]})$. A straightforward hybrid argument over the $\mathbf{c}_i$, based on the indistinguishability of $\mathcal{F}'_{\mathsf{RKA}[\Phi]}$, shows the indistinguishability of $\mathcal{F}_{\mathsf{RKA}[\Phi]}(C)$.

Theorem 17. *Let Σ' be a $\mathsf{RKA\text{-}KDM}[\Phi, \Psi]$-secure SKE scheme with an indistinguishable $\mathsf{RKA}[\Phi]$ oracle $\mathcal{F}_{\mathsf{RKA}[\Phi]}$. If Ψ covers projections, then Σ_{BHR} is an $\mathsf{RKA\text{-}KDM}[\Phi, \Psi_{\mathsf{bnd}(L)}]$-secure SKE for any arbitrary but fixed bound L.*

Proof. We only sketch the proof here, which is straightforward and based on a short sequence of games. Our first game is the original $\mathsf{RKA\text{-}KDM}[\Phi, \Psi]$ experiment (see Definition 1). In the next game, we no longer use the secret key itself to answer the RKA part of queries. More concretely, for a given RKA-KDM query (φ, ψ), we compute $C \leftarrow \mathsf{E}_k(\psi(k))$ and output $\mathcal{F}_{\mathsf{RKA}[\Phi]}(\varphi, C)$ instead of directly returning $\mathsf{E}_{\varphi(k)}(\psi(k))$. The indistinguishability of this game hop follows directly from the indistinguishability of $\mathsf{RKA}[\Phi]$. Finally, we can simply follow the strategy from [15], Theorem 15, to compute C. This strategy requires that the garbling scheme used to construct Σ_{BHR} is privacy preserving and projective.

Acknowledgements. The authors would like to thank Martijn Stam for useful discussions and Rafael Dowsley for kindling our interest in the topic. Furthermore, we would like to thank Viet Tung Hoang for pointing out a more efficient and less complicated way to achieve bounded-KDM security (based on [14]) than the one we first decided on (based on [6]).

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. Key-Dependent Message Security: Generic Amplification and completeness. In *EUROCRYPT*, pages 527–546, 2011.
[4] Benny Applebaum. Garbling XOR gates "For Free" in the Standard Model. In *TCC*, pages 162–181, 2013.
[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] Mihir Bellare, Viet Tung Hoang, and Phillip Rogaway. Foundations of garbled circuits. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 784–796. ACM, 2012.
[15] Mihir Bellare, Viet Tung Hoang, and Phillip Rogaway. Foundations of garbled circuits. Cryptology ePrint Archive, Report 2012/265, 2012. `http://eprint.iacr.org/`.
[16] Eli Biham. New types of Cryptoanalytic Attacks using Related Keys. In *EUROCRYPT*, pages 398–409, 1993.
[17] Eli Biham, Orr Dunkelman, and Nathan Keller. A Related-Key Rectangle Attack on the Full KASUMI. In *ASIACRYPT*, pages 443–461, 2005.
[18] Eli Biham, Orr Dunkelman, and Nathan Keller. Related-Key Impossible Differential Attacks on 8-Round AES-192. In *CT-RSA*, pages 21–33, 2006.
[19] Eli Biham, Orr Dunkelman, and Nathan Keller. A Simple Related-Key Attack on the Full SHACAL-1. In *CT-RSA*, pages 20–30, 2007.

[20] Alex Biryukov and Dmitry Khovratovich. Related-Key Cryptanalysis of the Full AES-192 and AES-256. In *ASIACRYPT*, pages 1–18, 2009.
[21] Alex Biryukov, Dmitry Khovratovich, and Ivica Nikolic. Distinguisher and Related-Key Attack on the Full AES-256. In *CRYPTO*, pages 231–249, 2009.
[22] 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.
[23] 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.
[24] Florian Böhl, Gareth T. Davies, and Dennis Hofheinz. Encryption schemes secure under related-key and key-dependent message attacks. *IACR Cryptology ePrint Archive*, 2013:653, 2013.
[25] Dan Boneh, Shai Halevi, Michael Hamburg, and Rafail Ostrovsky. Circular-secure encryption from Decision Diffie-Hellman. In *CRYPTO*, pages 108–125, 2008.
[26] 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.
[27] Zvika Brakerski, Shafi Goldwasser, and Yael Tauman Kalai. Black-Box Circular-Secure Encryption beyond Affine Functions. In *TCC*, pages 201–218, 2011.
[28] 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.
[29] Stefan Dziembowski and Krzysztof Pietrzak. Leakage-Resilient Cryptography. In *FOCS*, pages 293–302, 2008.
[30] Shafi Goldwasser and Silvio Micali. Probabilistic Encryption. *J. Comput. Syst. Sci.*, 28(2):270–299, 1984.
[31] Shai Halevi and Hugo Krawczyk. Security under Key-Dependent Inputs. In *ACM Conference on Computer and Communications Security*, pages 466–475, 2007.
[32] Dennis Hofheinz. Circular Chosen-Ciphertext Security with Compact Ciphertexts. In *EUROCRYPT*, pages 520–536, 2013.
[33] Dennis Hofheinz and Dominique Unruh. Towards Key-Dependent Message Security in the Standard Model. In *EUROCRYPT*, pages 108–126, 2008.
[34] Tal Malkin, Isamu Teranishi, and Moti Yung. Efficient Circuit-Size Independent Public Key Encryption with KDM Security. In *EUROCRYPT*, pages 507–526, 2011.
[35] Silvio Micali and Leonid Reyzin. Physically Observable Cryptography. In *TCC*, pages 278–296, 2004.
[36] Hoeteck Wee. Public Key Encryption against Related Key Attacks. In *Public Key Cryptography*, pages 262–279, 2012.