Relations among new CCA security notions for approximate FHE*

Sébastien Canard[1], Caroline Fontaine[2], Duong Hieu Phan[1], David Pointcheval[3], Marc Renard[4] and Renaud Sirdey[4]

[1] Télécom Paris, Institut Polytechnique de Paris, F-91120, Palaiseau, France,
sebastien.canard@telecom-paris.fr; hieu.phan@telecom-paris.fr
[2] Université Paris-Saclay, CNRS, ENS Paris-Saclay, Laboratoire Méthodes Formelles, 91190, Gif-sur-Yvette, France,
caroline.fontaine@cnrs.fr
[3] DIENS, École normale supérieure, CNRS, Inria, PSL University, Paris, France,
david.pointcheval@ens.fr
[4] Université Paris-Saclay, CEA, List, F-91120, Palaiseau, France,
marc.renard@cea.fr; renaud.sirdey@cea.fr

Abstract. In a recent Eurocrypt'24 paper, Manulis and Nguyen have proposed a new CCA security notion, vCCA, and associated construction blueprints to leverage both CPA-secure and correct FHE beyond the CCA1 security barrier. However, because their approach is only valid under the correctness assumption, it leaves a large part of the FHE spectrum uncovered as many FHE schemes used in practice turn out to be approximate and, as such, do not satisfy the correctness assumption. In this paper, we improve their work by defining and investigating a variant of their security notion which is suitable for a more general case where approximate FHE are included. As the passive security of approximate FHE schemes is more appropriately captured by CPA^D rather than CPA security, we start from the former notion to define our vCCA^D new security notion. Although, we show that vCCA and vCCA^D are equivalent when the correctness assumption holds, we establish that vCCA^D security is strictly stronger than vCCA security in the general case. In doing so, we interestingly establish several new separation results between variants of CPA^D security of increasing strength. This allows us to clarify the relationship between vCCA security and CPA^D security, and to reveal that the security notions landscape is much simpler for correct FHE than when approximate ones are included — in which case, for example, we establish that multiple challenges security notions are strictly stronger than single-challenge ones for both CPA^D and vCCA^D security. Lastly, we also give concrete construction blueprints, showing how to leverage some of the blueprints proposed by Manulis and Nguyen to achieve vCCA^D security. As a result, vCCA^D security is the strongest CCA security notion so far known to be achievable by both correct and approximate FHE schemes.

* This work was supported by the France 2030 ANR Projects ANR-22-PECY-003 SecureCompute.

Keywords: FHE · CPA^D · CCA security · SNARK · Verifiability.

1 Introduction

Since its inception more than ten years ago, Fully Homomorphic Encryption has been the subject of a lot of research toward more efficiency and better practicality. From a security perspective, however, FHE still raises a number of questions and challenges. In particular, all the FHE usable in practice, BFV [5,12], BGV [6], CKKS [9] and TFHE [10], achieve CPA security but are trivially CCA1 insecure. Although it is well-known that malleability is contradictory with CCA2 security, building efficient FHE constructions achieving some degree of CCA security (e.g. CCA1) remains a very important open challenge.

From a theoretical perspective, a significant step has been recently achieved by Manulis and Nguyen in [20] with the introduction of the notion of vCCA security, which is proven to be strictly stronger than CCA1 security while being achievable by FHE-based malleable schemes through several construction blueprints. In essence, these construction strategies consist in starting from a CPA secure and *correct* FHE and augmenting it with the machinery required for proving the well-formedness of *fresh* ciphertexts (i.e. ciphertexts which are direct outputs of the encryption function) as well as that of *evaluated* ciphertexts (i.e. ciphertexts derived from well-formed fresh ciphertexts by means of genuine homomorphic operations), with the decryption function of the augmented scheme returning $\perp$ when the proof verification fails. The intuition behind such construction strategies is that the proof machinery downgrades attackers to CPA ones and that, as a result, some form of CCA security is achieved by the augmented scheme. Although several techniques can be used to ensure the well-formedness of fresh ciphertexts (such as signatures in the private key setting, or Naor-Yung [21] in the public key setting), their approach intimately relies on Succinct Non-interactive Arguments of Knowledge (SNARKs) to enforce the well-formedness of evaluated ciphertexts. Under the assumption that the underlying SNARK is *simulation-sound extractable*, it then becomes possible to define a new (single challenge) security game along with a new security notion (vCCA), in the spirit of the CCA2 game: whereas the (second step) CCA2 game decryption oracle rejects the challenge ciphertext, the vCCA security game (second step) decryption oracle rejects all byproducts of the challenge ciphertext, identified by means of the SNARK extractor. One of Manulis and Nguyen's main contributions is to show, interestingly, that the resulting security notion, vCCA, is strictly stronger than CCA1 (no second step oracle) as well as a strict relaxation of CCA2 (because the CCA2 decryption oracle is more permissive than the vCCA decryption one). They also investigate the relationship between vCCA security and other CCA2 relaxations such as RCCA, CCA1.5, and others.

Another very important security notion for FHE, introduced by Li and Micciancio in [18], is that of CPA^D security, which formalizes the security of FHE against a slight and seemingly benign extension of CPA security where the adversary is granted access only to a highly constrained decryption oracle which

accepts only genuine ciphertexts, or ciphertexts derived from genuine ciphertexts by means of genuine homomorphic operations. The initial intuition is that, by knowing the cleartext inputs of an FHE calculation, the adversary should be able to compute all the outputs of that decryption oracle by his or herself and that, as a consequence, CPA^D security is implied by or even equivalent to CPA security. However, the correctness assumption implicitly lies at the heart of this reasoning and Li and Micciancio [18] demonstrated that these intuitions are not true for approximate FHE schemes such as CKKS for which it turns out that the CPA^D decryption oracle outputs leak the LWE noises in the ciphertexts, resulting in the ability for the adversary to easily and practically recover the secret decryption key of the scheme. Although initially introduced for approximate FHE, recent works [7,8] have shown that the non-approximate FHE schemes that were previously considered immune to CPA^D attacks are, contrary to this folklore belief, all CPA^D insecure as soon as decryption errors can or can be made to occur with a non-negligible probability.

In their paper, Manulis and Nguyen [20] define and study vCCA security only under the correctness assumption and address only very briefly CPA^D security, essentially claiming informally that their vCCA scheme construction blueprints also apply to approximate FHE "with the caveat that approximate FHE schemes need to be CPA^D-secure". In the present paper, we clarify the relationship between vCCA security and CPA^D security, and propose a new CCA security notion, vCCA^D, covering the spectrum of both correct *and* approximate FHE schemes. We show that both notions are equivalent when the correctness assumption holds, but establish that vCCA^D security is strictly stronger than vCCA security in the general case where approximate FHE are allowed. In doing so, we interestingly establish several new separation results between variants of CPA^D security of increasing strength. This allows us to show that vCCA security does not imply CPA^D security, but rather a much weaker single-challenge "CCA1 style" variant of it. We also reveal that the security notion landscape is much simpler for correct FHE than in the general case where, for example, we establish that multiple challenges security notions are strictly stronger than single-challenge ones for both CPA^D and vCCA^D security. Lastly, we also study concrete construction blueprints, showing how to leverage some of the blueprints proposed in [20] to achieve the new and stronger vCCA^D security.

Our first motivation for this study is practical: although the construction blueprints discussed in [20] and Sec. 6 may not be amenable to efficient implementations in their full generality, it seems possible to instantiate them in use-cases requiring only special classes of homomorphic calculations to be performed. When this is possible, vCCA and vCCA^D security provide a yardstick to achieve CCA security in a context where decryption oracles often naturally occur in many application scenarios for FHE. We elaborate more on this points in our concluding remarks (Sec. 7). Our second motivation is more theoretical, as this line of works allows to better understand and probe the limitations of FHE in terms of CCA security with, as we establish in this paper, vCCA^D security as the strongest CCA security notion so far known to be achievable by FHE in

the general regime where approximate/non-exact schemes are considered (with most practically used FHE schemes falling in that later category).

1.1 Summary of security notions and contributions

In this work, we study the following (non standard) security notions:

- CPA^D: the multiple challenges passive security notion introduced in [18] for approximate FHE.
- $\mathrm{CPA}_2^D \equiv \mathrm{CPA}_{\mathrm{SC}}^D$: restriction of CPA^D to the single challenge case.
- CPA_1^D: restriction of CPA_2^D with the decryption oracle closing after the challenge request (similar in spirit to the CCA1/CCA2 definitions). Note that CPA_1^D is different from non-adaptive CPA^D as defined and studied in [18].
- $\mathrm{vCCA}_{\mathrm{SC}}$: the single challenge CCA security notion introduced in [20] for correct FHE. Note that it is simply denoted vCCA in [20].
- vCCA: the multiple challenge variant of vCCA (this variant was not considered in [20]).
- vCCA^D: our main new multiple challenge CCA security notion for FHE in the general regime which includes approximate FHE.
- $\mathrm{vCCA}_{\mathrm{SC}}^D$: restriction of vCCA^D to the single challenge case.

Note that, following standard conventions [3], the multiple challenge notions will sometimes be prefixed by LOR- to avoid any ambiguity with the corresponding single challenge notions (also known as FTG).

With this in mind, the contributions of this paper are the following:

- When the correctness assumption holds for the underlying FHE, we show that:
  - CPA_1^D, $\mathrm{CPA}_2^D \equiv \mathrm{CPA}_{\mathrm{SC}}^D$ and CPA^D security are (unsurprisingly) all equivalent to CPA security.
  - In that regime we also show that $\mathrm{vCCA}_{\mathrm{SC}}$, vCCA, $\mathrm{vCCA}_{\mathrm{SC}}^D$ and vCCA^D security are also all equivalent.
- In the general case where the correctness assumption does not necessarily hold and approximate FHE are allowed, the picture we reveal is much more interesting:
  - For CPA^D security, we establish that $\mathrm{CPA}_1^D \prec \mathrm{CPA}_2^D \prec \mathrm{CPA}^D$ which, as a bonus, settles the question of the relationship between single and multiple-challenge CPA^D security that was left open in [18].
  - We clarify the relationship between vCCA and CPA^D security by showing that $\mathrm{CPA}_1^D \prec \mathrm{vCCA}_{\mathrm{SC}}$ but that $\mathrm{vCCA}_{\mathrm{SC}}$ security implies neither CPA_2^D nor CPA^D security (and vice-versa), contrary to what was informally claimed in [20].
  - For vCCA security, we further establish that $\mathrm{vCCA}_{\mathrm{SC}} \equiv \mathrm{vCCA}$ and that $\mathrm{vCCA}_{\mathrm{SC}} \prec \mathrm{vCCA}_{\mathrm{SC}}^D$, thus demonstrating that our new security notion is strictly stronger than vCCA security even in the single challenge case.

  - Lastly, for vCCA^D security, we prove that CPA^D<vCCA^D, and further prove that $\text{vCCA}^D_{\text{SC}}$<$\text{vCCA}^D$, which therefore implies that vCCA^D is the strongest of all these notions in the general FHE case and that it is the one that should be strived for.
- Lastly, we revisit the CPA-to-vCCA FHE scheme construction blueprints proposed in [20] under the correctness assumption and turn them, when possible, into CPA^D-to-vCCA^D blueprints. In particular, we are able to do so and prove the vCCA^D security of the (private key, designated verifier) Encrypt-then-MAC, (private key, public verifier) Encrypt-then-Sign, and (public key, designated verifier) CCA2-Companion-Ciphertext blueprints; but we also show that the (public key, public verifier) Naor-Young-based blueprint cannot be used when the correctness assumption does not hold. In this later case (public key, public verifier), we thus propose a new blueprint which achieves vCCA^D (and vCCA) security in the general setting where the correctness assumption does not necessarily hold.

Figure 1 summarizes the relationships between these notions in the general case. When proving relationships between security notions, we make a difference between the *correct case* or *correct regime*, where the FHE correctness assumption is assumed to hold, and the *general case* or *general regime*, where approximate FHE are allowed. This terminology is used consistently in the paper.

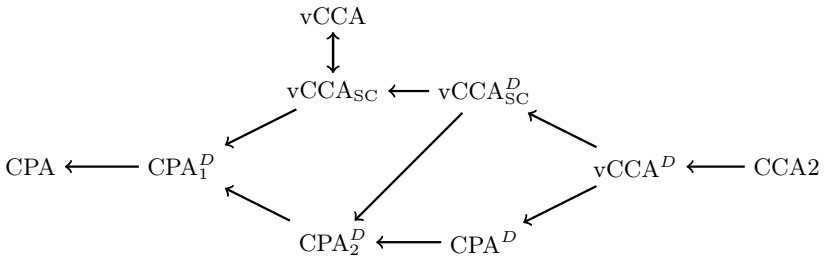

Fig. 1. Summary of the security notions investigated in this paper and their relationships in the general regime where approximate FHE are allowed. Note that all single arrows are strict implications, and remind that $\text{CPA}^D_2 \equiv \text{CPA}^D_{\text{SC}}$ is the restriction of CPA^D to the single challenge case and that CPA^D_1 is the restriction of CPA^D_2 with the decryption oracle closing after the challenge request. Please also remind that notions without a subscript in their names are multiple challenge ones and that, for consistency, we denote by vCCA_{SC} the single challenge security notion defined in [20].

1.2 Paper organization

This paper is organized as follows. After some preliminaries (Sect. 2), Sect. 3 introduces the definition of vCCA^D security and recalls the definitions of CPA^D

and vCCA security. It also investigates the definitional connexions between these notions. Then, in Sect. 4, we investigate the relationship among the single challenge variants of these security notions in both the restricted setting where the correctness assumption holds and in the general case where approximate FHE are allowed. Then, in Sect. 5, we focus on unveiling the relationships between the single and multiple-challenge variants of these security notions as well as the relationships between the multiple-challenge variants between each other. Sect. 6 is devoted to prove the security of several generic scheme construction blueprints with respect to the stronger multiple challenge vCCA^D security notion. Sect. 7 then concludes the paper.

2 Preliminaries

We define an encryption scheme $\mathcal{E} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ over key space $\mathcal{K}$, plaintext domain $\mathcal{P}$ and ciphertext domain $\mathcal{C}$ as a triplet of PPT algorithms:

- KeyGen: which, on input 1^λ, outputs an encryption key ek and a decryption key sk.
- $\mathsf{Enc}_{\mathsf{ek}}$: which, on inputs $m \in \mathcal{P}$ and the encryption key ek, outputs an encryption $c \in \mathcal{C}$ of m.
- $\mathsf{Dec}_{\mathsf{sk}}$: which, on inputs $c \in \mathcal{C}$ and the decryption key sk, outputs a decryption $m \in \mathcal{P} \cup \{\perp\}$ of c.

Let COIN denote the randomness space of $\mathcal{E}$, we will sometimes externalize the randomness used in the encryption function by means of the notation $\mathsf{Enc}_{\mathsf{ek}}(m; r)$, with $m \in \mathcal{P}$ and $r \in \mathsf{COIN}$ (in this case, the function $\mathsf{Enc}_{\mathsf{ek}} : \mathcal{P} \times \mathsf{COIN} \longrightarrow \mathcal{C}$ is deterministic). When ek is public, we say that $\mathcal{E}$ is a *public-key* encryption scheme. Conversely, when ek has to remain private and an adversary can create valid ciphertexts with at most $\mathrm{neg}(\lambda)$ probability using only public knowledge, we say that $\mathcal{E}$ is a *private-key* encryption scheme. When for all $(\mathsf{ek}, \mathsf{sk}) \in \mathcal{K}$ and all $m \in \mathcal{P}$ we have that

$$\Pr_{r \in \mathsf{COIN}}(\mathsf{Dec}_{\mathsf{sk}}(\mathsf{Enc}_{\mathsf{ek}}(m; r)) \neq m) \leq \mathrm{neg}(\lambda), \tag{1}$$

we say that $\mathcal{E}$ is *correct* (when the above equality always holds, we will talk about *perfect* correctness). A ciphertext is *valid* if it is the output of the encryption function for some message $m \in \mathcal{P}$, that is, if there exists $m \in \mathcal{P}$ and some randomness $r \in \mathsf{COIN}$ such that $c = \mathsf{Enc}_{\mathsf{ek}}(m; r)$. We further say that $\mathcal{E}$ is *verifiable* if there exists a PPT algorithm Verif, taking a ciphertext as input, which tells whether or not this ciphertext is valid with a $\mathrm{neg}(\lambda)$ probability of error for an adversary with knowledge of only public data. For verifiable schemes, the decryption function with input ciphertext c outputs $\perp$ when $\mathsf{Verif}(c) = \mathsf{False}$. Note that for all non-homomorphic schemes considered in this paper, $\mathsf{Dec}_{\mathsf{sk}}$ will always be a *deterministic* polynomial-time algorithm. When there is no ambiguity, we omit the ek and sk subscripts to Enc and Dec to lighten the notation.

Given a function class $\mathcal{F}_H$, we define an homomorphic encryption (HE) scheme $\mathcal{E}_H$ as an encryption scheme augmented by a *deterministic*[1] polynomial-time algorithm Eval which, on input $f \in \mathcal{F}_H$ and $c_1, ..., c_K \in \mathcal{C}^K$ (where K denotes the arity of function f), outputs a new *evaluated* ciphertext. When $\mathcal{E}_H$ satisfies condition (1) and when Eval is such that for all $(\mathsf{ek}, \mathsf{sk}) \in \mathcal{K}$, all $f \in \mathcal{F}_H$ and all $m_1, ..., m_K \in \mathcal{P}^K$

$$\Pr_{\vec{r} \in \mathsf{COIN}^K}(\mathsf{Dec}(\mathsf{Eval}(f, \mathsf{Enc}(m_1; r_1), ..., \mathsf{Enc}(m_K; r_K))) \neq f(m_1, ..., m_K)) \leq \mathrm{neg}(\lambda),$$

we say that $\mathcal{E}_H$ is a *correct* HE scheme. When this is not the case, we say that $\mathcal{E}_H$ is an *approximate* HE scheme. Consistently with [19], to avoid arbitrary schemes with unreliable Eval to be marketed as approximate HE schemes, we add an additional condition that, for some (small) $\varepsilon \geq 0$, the following holds

$$\Pr_{\vec{r} \in \mathsf{COIN}^K}(\|\mathsf{Dec}(\mathsf{Eval}(f, \mathsf{Enc}(m_1; r_1), ..., \mathsf{Enc}(m_K; r_K))) - f(m_1, ..., m_K)\|_\infty \leq \varepsilon) \geq p_\varepsilon, \tag{2}$$

with $p_\varepsilon \geq \frac{3}{4}$[2].

When $\mathcal{E}_H$ achieves correctness only for $\mathcal{F}_C \subset \mathcal{F}_H$, it is said to be $\mathcal{F}_C$-*correct* (in the spirit of [1]).

All the HE schemes we consider in this paper are public-key. Also note that for the homomorphic schemes considered in this paper, $\mathsf{Dec}_{\mathsf{sk}}$ is by default a *deterministic* polynomial-time algorithm, unless explicitly stated otherwise (e.g. CKKS with noise flooding as defined in [19] has a probabilistic decryption algorithm). When $\perp \in \mathcal{E}_H.\mathcal{P}$, we will further always assume a *consistency* property which requires that $\forall \vec{m}, \vec{r} \in \mathcal{P}^K \times \mathsf{COIN}^K$,

$$\mathsf{Dec}(\mathsf{Eval}(f, \mathsf{Enc}(m_1; r_1), ..., \mathsf{Enc}(m_K; r_K))) \neq \perp, \tag{3}$$

and

$$\mathsf{Dec}(\mathsf{Eval}(f, c_1, ..., c_K))) = \perp, \tag{4}$$

whenever $\exists i : \mathsf{Dec}(c_i) = \perp$.

As in [20], for signatures and MAC we use the standard definitions respectively $\Sigma = (\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$ and $M = (\mathsf{KeyGen}, \mathsf{Tag}, \mathsf{Verify})$ and assume SUF-CMA security. In our case, EUF-CMA security will not be sufficient because we essentially use signatures as a building block for CCA2 encryption schemes in the private key setting. Lastly, we consider straightline-extractable SNARK, $\Pi = (\mathsf{Setup}, \mathsf{Prove}, \mathsf{Verify})$, over function class $\mathcal{F}_E$ (slightly departing from [20] which required simulation-sound extractability). Indeed, in the security proofs of the constructions we study in Sect. 6, we are in the setup where only the adversary generates proofs and where our simulator only invokes the SNARK

[1] As is the case for the mainstream FHE schemes such as BFV, BGV, TFHE and even CKKS.

[2] We use this probability only to prove non-negligible advantages in some of our proofs. In practice p_ε is typically chosen above $1 - 2^{-40}$. In some contexts, e.g. [1], p_ε even has to be at least $1 - \mathrm{neg}(\lambda)$.

extractor when $\Pi.\mathsf{Verify}(\pi) = \mathsf{True}$ on a proof π. Additionally, because we do not investigate circuit privacy, we do not need zk-SNARKs. Formal definitions for these notions are recalled in appendix A.

3 Defining vCCA^D security

This section introduces our vCCA^D security notion which is an extension of both vCCA and CPA^D (hence the name). As they both are extensively referred to in this paper, we start by recalling the games associated with these two notions. We then define the vCCA^D game.

3.1 The CPA^D game

The CPA^D game has been introduced in the context of approximate FHE. CPA^D security is a slight extension of CPA security defined by the following Left-Or-Right multiple challenge security game.

Given an homomorphic encryption scheme

$$\mathcal{E}_H = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval}),$$

an adversary $\mathcal{A}$ and value λ for the security parameter, the game is parameterized by a bit $b \xleftarrow{\$} \{0,1\}$, unknown to $\mathcal{A}$, and an initially empty state S of message-message-ciphertext triplets:

- Key generation: Run $(\mathsf{ek}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$, and give ek to $\mathcal{A}$ (when the scheme is public-key).
- Encryption request: When $\mathcal{A}$ queries $(\texttt{plaintext}, m)$, $m \in \mathcal{P}$ compute $c = \mathsf{Enc}(m)$, give c to $\mathcal{A}$ and do
$$S := [S; (m, m, c)].$$
- Challenge request: When $\mathcal{A}$ queries $(\texttt{test messages}, m_0, m_1)$, $m_0, m_1 \in \mathcal{P}^2$ $(m_0 \neq m_1)$ compute $c = \mathsf{Enc}(m_b)$, give c to $\mathcal{A}$ and do
$$S := [S; (m_0, m_1, c)].$$
- Evaluation request: When $\mathcal{A}$ queries $(\texttt{eval}, f, l_1, \ldots, l_K)$ $(l_i \in \{1, ..., |S|\}, \forall i)$, compute
$$m'_0 = f(S[l_1].m_0, \ldots, S[l_K].m_0),$$
and
$$m'_1 = f(S[l_1].m_1, \ldots, S[l_K].m_1),$$
as well as
$$c' = \mathsf{Eval}(f, S[l_1].c, \ldots, f[l_K].c),$$
give c' to $\mathcal{A}$ and do
$$S := [S; (m'_0, m'_1, c')].$$

- Decryption request: When $\mathcal{A}$ queries $(\texttt{ciphertext}, l)$ ($l \in \{1, ..., |S|\}$) proceed as follows: if $S[l].m_0 \neq S[l].m_1$ then return $\perp$ to $\mathcal{A}$, otherwise return her $\mathsf{Dec}(S[l].c)$.
- Guessing stage (after polynomially many interleaved encryption and decryption requests): When $\mathcal{A}$ outputs $(\texttt{guess}, b')$, the outcome of the game is determined as follows. If $b' = b$ then $\mathcal{A}$ wins the game. Otherwise, $\mathcal{A}$ loses the game.

A number of points should be emphasized with respect to the above game. First, the decryption oracle accepts only ciphertexts from the game state which are necessarily well-formed (either produced by an encryption or challenge request, or derived by the evaluation oracle via an evaluation request i.e., derived by correctly applying homomorphic operators to well-formed ciphertexts). As such, the above game thus does not capture any CCA aspects. Second, when $S[l].m_0 = S[l].m_1$ it is important that the decryption oracle returns $\mathsf{Dec}(S[l].c)$ and not $S[l].m_0$ (or, equivalently in that case, $S[l].m_1$). For correct FHE, this has no impact, as $\mathsf{Dec}(S[l].c) = S[l].m_0 = S[l].m_1$ in that case (and, as $\mathcal{A}$ learns nothing it does not already know, CPA^D security coincides with CPA security for correct FHE). For approximate FHE, however, even when $S[l].m_0 = S[l].m_1$, we have (with overwhelming probability) that $\mathsf{Dec}(S[l].c) \neq S[l].m_0$ and $\mathsf{Dec}(S[l].c) \neq S[l].m_1$. Thus for approximate FHEs, the decryption oracle grants $\mathcal{A}$ access to information she cannot compute on her own, resulting or not in a guessing advantage depending on whether or not the cryptosystem at hand is CPA^D secure. Additionally, let us also emphasize that, in the above game, $\mathcal{A}$ has control on the homomorphic calculations that are performed as f is included in the evaluation request. As a last remark, we acknowledge the fact that explicitly adding encryption requests to the above game is redundant as these are simply challenge requests with $m_0 = m_1$ (as was assumed in the original definition of [18]). However, since we are going back and forth between single and multiple challenges security notions in the sequel, we feel that this explicitation may avoid later confusions. Although the number of allowed challenge requests may vary from one security notion to another, the number of encryption requests an adversary can perform always remains "unlimited".

In addition to the above multiple-challenge notion initially defined in [18], we also define and consider the following weaker restrictions of it:

- $\mathrm{CPA}_2^D \equiv \mathrm{CPA}_{\mathrm{SC}}^D$: restriction of CPA^D to the single challenge case where the adversary is allowed only one request of the form $(\texttt{test messages}, m_0, m_1)$ with $m_0 \neq m_1$.
- CPA_1^D: restriction of CPA_2^D with the decryption oracle closing after the challenge request (similar in spirit to the CCA1/CCA2 definitions, hence the choice for the notations).

Note that CPA_1^D is different from non-adaptive CPA^D as defined and studied in [18]. Indeed, there is a slight difference between the notion of adaptability as understood in the multiple-challenge context of [18] (the adversary performs all

its requests at once) and that which is usually assumed between single-challenge CCA1 and CCA2 (the adversary performs all its decryption requests before the *unique* challenge ciphertext is published).

3.2 The vCCA game

We now consider the vCCA game as recently introduced in [20]. Contrary to the CPA^D game presented in the previous section, that game is *single challenge* meaning that the adversary performs only one request to the challenge oracle with $m_0 \neq m_1$. As already stated in Sect. 1.1, we will now consistently refer to the original game and security notion in [20] as $\mathrm{vCCA}_{\mathrm{SC}}$ and reserve the vCCA naming for its multiple challenge generalisation which we introduce and study in Sect. 5. Also, in the $\mathrm{vCCA}_{\mathrm{SC}}$ security game, the cryptosystem is augmented with a PPT witness extractor $\mathsf{Extract} : \mathcal{C} \times \mathcal{X} \longrightarrow \mathcal{F}_E \cup \{\mathsf{id}\} \times \mathcal{C}^*$, where $\mathcal{X}$ denotes a set of auxiliary data, such that:

- For any ciphertext $c \in \mathcal{C}$ which is obtained by invoking $\mathsf{Eval}(f, c_1, ..., c_K)$,

$$\mathsf{Extract}(c, \mathsf{aux}) = (f, c_1, ..., c_K).$$

- Otherwise, $\mathsf{Extract}(c, \mathsf{aux}) = (\mathsf{id}, c)$.

Let us emphasize that all the construction blueprints which will be discussed in Sect. 6 embed proof material in their ciphertexts and rely on a SNARK to enforce correct homomorphic evaluations over some input ciphertexts, Intuitively, the above $\mathsf{Extract}$ thus corresponds to the extractor of that underlying SNARK which allows to retrieve a witness from the proven statement as well as auxiliary data forming the trace of the execution of the adversary (as formally defined in Sect. A). Because such an extractor exists only with respect to provers able to produce valid proofs, we will further assume, in the case of Designated-Verifier SNARKs, that the adversary is given access to a verification oracle. By abuse of notations we will omit the aux argument in the sequel.

In particular, the above definition implies that

$$\mathsf{Extract}(\mathsf{Eval}(f, \mathsf{Enc}(m_1, r_1), ..., \mathsf{Enc}(m_K, r_K))) = (f, \mathsf{Enc}(m_1, r_1), ..., \mathsf{Enc}(m_K, r_K)). \tag{5}$$

By extension, we also expect that

$$\mathsf{Extract}(\mathsf{Enc}(m, r)) = (\mathsf{id}, \mathsf{Enc}(m, r)). \tag{6}$$

Being single challenge, the $\mathrm{vCCA}_{\mathrm{SC}}$ game therefore has two decryption oracles[3]. Before the unique challenge encryption oracle request, the first step decryption oracle is simply as follows:

- Decryption request (first step): When $\mathcal{A}$ queries $(\texttt{ciphertext}, c)$ proceed as follows: return her $\mathsf{Dec}(c)$.

[3] Of course, the $\mathrm{vCCA}_{\mathrm{SC}}$ game has no evaluation oracle as the adversary performs the homomorphic evaluations on its own in both the private and public key setting.

Then, after challenge generation,

- Decryption request (second step): When $\mathcal{A}$ queries $(\texttt{ciphertext}, c)$ proceed as follows:
  1. Let
  $$(f, c_1, ..., c_K) = \mathsf{Extract}(c),$$
  if
  $$c^* \in \{c_1, ..., c_K\} \tag{7}$$
  then return $\perp$ to $\mathcal{A}$.
  2. Otherwise return her $\mathsf{Dec}(c)$.

where c^* is the challenge ciphertext. As such, the vCCA_{SC} game is exactly the single challenge CCA2 game, with the second step decryption oracle being augmented with case 1 above (which, in essence, filters out *all* byproducts of the challenge ciphertext). Let us emphasize that vCCA_{SC} security is defined and investigated in [20] only under the (strong) assumption that S is *correct*. However, let us also emphasize that *the correctness assumption plays no role in the above definition which remains meaningful in the general regime where approximate FHE are allowed*.

As a last comment, let us emphasize that, although its definition seems intrinsically single-hop (e.g., limited to one homomorphic evaluation over fresh ciphertexts), vCCA_{SC} security can, at least in principle, be extended to the multi-hop setting by allowing recursive calls to $\mathsf{Extract}$ [20, Remark 2, p. 28]. Still, as emphasized in [20] and later in Sect. 6, coming up with practically credible constructions for achieving vCCA security limited to the single-hop setting is already quite challenging yet sufficient to cover a wide range of FHE use-cases.

3.3 vCCA^D security: definitions and first properties

Contrary to the original vCCA security game introduced and studied in [20] (which, again, we refer to as vCCA_{SC} in this paper), the vCCA^D game is a multiple challenge one. Due to subtleties that will soon be clear, *we first define it in the private key setting*, starting from the CPA^D game in Sect. 3.1 *without the evaluation oracle* and assuming, as in vCCA_{SC}, the existence of the same extractor.

In the private key setting, the vCCA^D game decryption oracle is defined as:

- Decryption request: When $\mathcal{A}$ queries $(\texttt{ciphertext}, c)$ proceed as follows:
  1. Let
  $$(f, c_1, ..., c_K) = \mathsf{Extract}(c),$$
  if
  $$f(\text{left}(c_1), ..., \text{left}(c_K)) \neq f(\text{right}(c_1), ..., \text{right}(c_K)) \tag{8}$$
  then return $\perp$ to $\mathcal{A}$.
  2. Otherwise return her $\mathsf{Dec}(c)$.

Where for any ciphertext $c \in \mathcal{C}$ we define

$$\text{left}(c) = \begin{cases} S[i].m_0 \text{ if } \exists i : S[i].c = c, \\ \perp \qquad \text{otherwise,} \end{cases} \tag{9}$$

as well as,

$$\text{right}(c) = \begin{cases} S[i].m_1 \text{ if } \exists i : S[i].c = c, \\ \perp \qquad \text{otherwise,} \end{cases} \tag{10}$$

and with the convention that $f(m_1, ..., m_K) = \perp$ when $\exists i : m_i = \perp$. Note that if the left and right evaluations both give $\perp$, condition (8) is not satisfied and $\mathsf{Dec}(c)$ is returned to $\mathcal{A}$.

Remark 1. It is clear that any ciphertext accepted by the vCCA^D game decryption oracle is also accepted by the LOR-CCA2 game one but not vice-versa. For example, ciphertext $\mathsf{Eval}(\text{sum}, c^*, \mathsf{Enc}(1))$ is accepted by the LOR-CCA2 decryption oracle (but rejected by the vCCA^D one) and trivially allows an adversary to win the CCA2 game. It follows that vCCA^D security is a strict relaxation of CCA2 security (which is well-known to exclude malleability[4]). †

Remark 2. In the private key setting, well-formed fresh ciphertexts (including challenge ones) can only be obtained by means of (encryption or challenge) oracle requests. Therefore, all such ciphertexts are registered in the game state S. It then follows that for any ciphertext of the form

$$c = \mathsf{Eval}(f, \mathsf{Enc}(m_1), ..., \mathsf{Enc}(m_K))$$

we have that $\text{left}(c) \neq \perp$ and $\text{right}(c) \neq \perp$. However, when the correctness assumption does not hold, we may have that $\mathsf{Dec}(c) \neq f(\text{left}(c_1), ..., \text{left}(c_K))$ as well as $\mathsf{Dec}(c) \neq f(\text{right}(c_1), ..., \text{right}(c_K))$. †

If we compare the vCCA$_{\text{SC}}$ game in previous Sect. 3.2 and the single challenge variant, vCCA$^D_{\text{SC}}$, of the above game, vCCA$_{\text{SC}}$'s second step oracle filters out *all* byproducts of the challenge ciphertext whereas (single challenge) vCCA$^D_{\text{SC}}$ filters out only those byproducts which allow to disciminate which of the two challenge plaintexts was encrypted.

Remark 3. From the definition of the two games, it is clear that all the ciphertexts accepted by the vCCA$_{\text{SC}}$ decryption oracle are also accepted by the vCCA$^D_{\text{SC}}$ one (but not vice-versa). There are indeed two types of ciphertexts which are rejected by the vCCA$_{\text{SC}}$ decryption oracle but accepted by the vCCA$^D_{\text{SC}}$ one:

[4] Additionally, it is well known that LOR-CCA2 security is equivalent to (single challenge) CCA2 (a.k.a., FTG-CCA2) in both the public key [4] and private key [3] settings. Also, note that CCA1 obviously does not really make sense in the multiple challenge setting.

1. Ciphertexts obtained through a legit call to Eval over well-formed fresh ciphertexts (with one of them being the challenge ciphertext) for which condition (8) does not hold, e.g. $\mathsf{Eval}(f, c^*, \mathsf{Enc}(m_2), ..., \mathsf{Enc}(m_K))$ with
$$f(m_0^*, m_2, ..., m_k) = f(m_1^*, m_2, ..., m_k),$$
where m_0^* and m_1^* denote the two challenge plaintexts. For example, ciphertext $\mathsf{Eval}(\text{mul}, c^*, \mathsf{Enc}(0))$ fall into this category.
2. Ciphertexts obtained through a legit call to Eval over arbitrary ciphertexts, with one of them being the challenge ciphertext and at least one of the others being ill-formed.

†

Throughout this paper and in particular in the separation results we establish, we (almost) always exploit the first of the above two gaps. As will be seen in Sect. 6, the second gap will be closed in the construction themselves by including the machinery necessary for the decryption *function* of the proposed schemes to reply $\perp$ when given either an ill-formed ciphertext or an evaluated ciphertext over non well-formed ones.

Defining vCCA^D security in the public key case. In the public key setting, the adversary can generate well-formed fresh ciphertexts independent of the challenge on his or her own. So only challenge-dependent fresh ciphertexts are guaranteed to be registered in the game state. In order to perform the left and right cleartext evaluations we therefore need a mean to access the messages that were given as inputs to the encryption function for well-formed ciphertexts that the adversary generated by his or herself. Note that, when the correctness assumption does not hold (which is also the regime under which we are willing to operate in this paper), these inputs cannot be recovered by merely decrypting those ciphertexts within the vCCA^D game decryption oracle.

Therefore, to define the vCCA^D game in the public key setting we need an additional extractor, denoted $\mathsf{Extract}'$, for recovering the encryption function inputs for fresh well-formed ciphertexts i.e.,
$$\mathsf{Extract}'(c) = \begin{cases} (m; r) & \text{when } c := \mathsf{Enc}(m, r), \\ \perp & \text{otherwise.} \end{cases} \tag{11}$$

Following this, *in the public key setting*, the vCCA^D game decryption oracle is then defined similarly to the private key case but with the notable difference that the left and right functions are replaced by the left$'$ and right$'$ functions defined as
$$\text{left}'(c) = \begin{cases} S[i].m_0 & \text{if } \exists i : S[i].c = c, \\ \mathsf{Extract}'(c).m & \text{otherwise,} \end{cases}$$
as well as,
$$\text{right}'(c) = \begin{cases} S[i].m_1 & \text{if } \exists i : S[i].c = c, \\ \mathsf{Extract}'(c).m & \text{otherwise.} \end{cases}$$

Following this, we however emphasize that, as we shall later see in Sect. 6, among the two public key vCCA_{SC} scheme construction blueprints considered in [20], only the one in which fresh ciphertexts are defined as the association of a FHE ciphertext encrypting m by means of randomness r and another ciphertext encrypting the concatenation of m and r under a CCA2-secure encryption scheme is applicable in the general case where the correctness assumption may not hold. In this approach the well-formedness of fresh ciphertext is verified by first decrypting the companion CCA2 ciphertext to recover m and r and then checking that the associated FHE ciphertext is indeed equal to $\mathcal{E}_H.\mathsf{Enc}(m, r)$. This, in essence, provides the additional extractor, $\mathsf{Extract}'$, expected in the above definition.

vCCA^D security vs CPA^D security. As a warm-up, let us now prove a first separation result between CPA^D and vCCA^D security.

Lemma 4. *vCCA^D security implies CPA^D security.*

Proof. By definition of the two games, the result of any encryption or decryption request performed by a CPA^D adversary is also accessible to a vCCA^D adversary. □

Proposition 5 (CPA^D $\not\Rightarrow$ vCCA^D). *If there exists a vCCA^D-secure scheme S, then there exists a scheme S' which is CPA^D-secure but not vCCA^D-secure.*

Proof. Let us start from a vCCA^D-secure scheme $S = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval})$. We now consider the scheme S' which is exactly S except that we modify the decryption function such that it leaks sk for a given randomly chosen input $c^{\triangle} \in \mathcal{C}$ i.e.,

$$\mathsf{Dec}'(c) = \begin{cases} \mathsf{sk} & \text{if } c = c^{\triangle}, \\ \mathsf{Dec}(c) & \text{otherwise.} \end{cases}$$

Additionally, S' public material now includes $c^{\triangle}$. The CPA^D security of S' then follows from the CPA^D security of S (by Lemma 4) as well as the fact that the CPA^D game decryption and evaluation oracles take state indices rather than ciphertexts as argument. As a consequence, a CPA^D adversary against S' cannot add $c^{\triangle}$ (or any byproduct of $c^{\triangle}$ obtained by means of homomorphic operations) to the game state (with non-negligible probability). Yet, S' is trivially vCCA^D-insecure, as a vCCA^D adversary against S' can submit $c^{\triangle}$ to the vCCA^{D}game decryption oracle and get sk in return. □

This simple proof pattern will occur several times in this paper.

4 Relations among the single challenge notions

We consider in this section the single challenge variants of vCCA^D and vCCA which we respectively denote $\text{vCCA}^D_{\text{SC}}$ and vCCA_{SC}. Following Sect. 3.2, in these

single challenge variants, we allow only one challenge request with $m_0 \neq m_1$. The challenge ciphertext and the associated messages are respectively denoted c^*, m_0^* and m_1^*. We further consider in this section the single challenge variant of CPA^D which we denote $\mathrm{CPA}^D_{\mathrm{SC}}$. In the single challenge case, we can further meaningfully split $\mathrm{CPA}^D_{\mathrm{SC}}$ in CPA^D_1 and $\mathrm{CPA}^D_2 \equiv \mathrm{CPA}^D_{\mathrm{SC}}$. Analogously to the distinction between CCA1 and CCA2, in CPA^D_1, the $\mathrm{CPA}^D_{\mathrm{SC}}$ decryption oracle closes after the challenge request is performed.

4.1 Relations between single-challenge variants of CPA^D

Because CPA^D security collapses onto CPA security in the correct regime, then CPA^D_1 is equivalent to CPA^D_2 in that regime. In the general regime, however, we have the following separation result (considering that CPA^D_2 trivially implies CPA^D_1).

Proposition 6 ($\mathrm{CPA}^D_1 \not\Longrightarrow \mathrm{CPA}^D_2$). *If there exists an FHE scheme S which is CPA^D_2-secure, then there exists an FHE encryption scheme S' which is CPA^D_1-secure but CPA^D_2-insecure.*

Proof. Let us consider a CPA^D_2-secure FHE scheme $S = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval})$. Consider the approximate scheme $S' = (\mathsf{KeyGen}', \mathsf{Enc}', \mathsf{Dec}', \mathsf{Eval}')$ built from S such that

$$\mathsf{Enc}'(m) = \mathsf{Enc}(m + g(m)),$$

where g is some function such that $g(0) \neq 0$, and KeyGen', Dec' and Eval' are similar to those of S.

S' is CPA^D_1-secure. This follows from the CPA^D_2 security of S and the fact that the approximation noise $g(m)$ is independent of S secret key material (which is the only information not available to a CPA^D_1 adversary).

S' is not CPA^D_2-secure. The adversary issues the *unique* encryption request with $m_0 \neq m_1$ to get

$$m_0^*, m_1^*, \mathsf{Enc}'(m_b^*),$$

say with $m_0^* = 0$ and $m_1^* = K$. He or she subsequently asks for an encryption of 0, c_0, and then asks for the computation of

$$c_{\mathrm{mul}} = \mathsf{Eval}'(\mathrm{mul}, c_0, c^*)$$

which the CPA^D_2 decryption oracle accepts as it is associated to the triplet $(0, 0, c_{\mathrm{mul}})$ in the game state (c_{mul} is an encryption of 0 with respect to S'). Now, recall the definition of ε and p_ε in Eq. 2 (p. 7). Then, assuming that the adversary has chosen K such that

$$\|g(0)^2 - (K + g(K))g(0)\|_\infty > 2\varepsilon, \tag{12}$$

he or she can decide that $b = 0$ when

$$\|\mathsf{Dec}'(c_{\mathrm{mul}}) - g(0)^2\|_\infty \leq \varepsilon$$

and $b = 1$ otherwise, and win the CPA^D_2 game with with probability at least p_ε. □

As an informal illustrative example for the above proof (assuming for simplicity sake $\mathcal{P} = \mathbb{Z}_t$, for some plaintext modulus $t >> \varepsilon$), we can choose $g(m) = 1$ for all m. So, when $b = 0$, $\mathsf{Dec}(c_{\text{mul}})$ falls in $I_0 = [1 - \varepsilon, 1 + \varepsilon]$ and when $b = 1$ it falls in $I_K = [K + 1 - \varepsilon, K + 1 + \varepsilon]$. Then, if we choose $m_1^* = K > 2\varepsilon$, we get $I_0 \cap I_K = \varnothing$, ensuring condition (12) above.

Note that this result is different from Proposition 2 in [18] which establishes that there exists (approximate) FHE schemes which are non-adaptive CPA^D secure while being adaptive CPA^D insecure. Indeed, as already pointed in Sect. 3.1, there is a slight difference between the notion of adaptability as understood in the multiple-challenge context of [18] (the adversary performs all its requests at once) and that which is usually assumed between single-challenge CCA1 and CCA2 (the adversary performs all its decryption requests before the challenge is published).

4.2 Relations between vCCA$_{\text{SC}}$ and single-challenge variants of CPA^D

Let us emphasize that the issue of approximate schemes is only succinctly and informally discussed in [20]. Indeed, from a construction point of view, that paper claims to define blueprints for constructing vCCA-secure schemes from "state-of-the-art FHE such as TFHE or CKKS with the caveat that approximate FHE schemes need to be CPA^D-secure"[5]. It turns out that the results in this section clarify the relationship between vCCA$_{\text{SC}}$ security and CPA^D security in the general regime where approximate FHE are allowed: vCCA$_{\text{SC}}$ in fact requires much less than full-blown CPA^D security but rather its weaker "CCA1 style" variant, CPA$_1^D$. Implicitly, we consider here a generalization of vCCA$_{\text{SC}}$ security beyond the correctness assumption. However, as argued in Sect. 3.2, in terms of security game definition, there is no dependency on the correctness assumption. Indeed, in [20], that assumption only steps in for proving the vCCA$_{\text{SC}}$ security of the proposed constructions.

Proposition 7. *vCCA$_{\text{SC}}$ security implies CPA$_1^D$ security.*

Proof. By definition, a CPA$_1^D$ adversary can only perform decryption requests which are independent of the challenge ciphertext. It thus follows that any request performed by a CPA$_1^D$ adversary can also be performed by a vCCA$_{\text{SC}}$ one. □

Proposition 8 (vCCA$_{\text{SC}}$ $\not\Longrightarrow$ CPA$_2^D$). *If there exists a vCCA$_{\text{SC}}$-secure scheme S, then there exists a scheme S' which is vCCA$_{\text{SC}}$-secure and CPA$_2^D$-insecure.*

Proof. We proceed similarly to the proof of Proposition 6. Let us start from a vCCA$_{\text{SC}}$-secure scheme $S = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval})$ from which we build the

[5] Following the recent attacks in [7,8], the authors of [20] further updated their ePrint version to put additional emphasis on the FHE correctness assumption (see Remark 1 on p. 5 and Sect. 5.4).

scheme S' with the only modification that

$$\mathsf{Enc}'(m) = \mathsf{Enc}(m + g(m)).$$

with g as in the proof of Proposition 6.
S' is $vCCA_{\mathrm{SC}}$-secure. Let $\mathcal{A}$ be a successful adversary against the $\mathrm{vCCA}_{\mathrm{SC}}$ security of S'. It is then easy to build an adversary $\mathcal{B}$ against the $\mathrm{vCCA}_{\mathrm{SC}}$ security of S. Indeed, $\mathcal{B}$ simulates $\mathcal{A}$ encryption and challenge requests simply by adding $g(m)$ to m. All other requests are transferred "as is" by $\mathcal{B}$ to the $\mathrm{vCCA}_{\mathrm{SC}}$ game against S.
S' is CPA_2^D-insecure. Identical to proof of Proposition 6: the CPA_2^D decryption oracle accepts the c_{mul} ciphertext since it is duly registered in the game state within the triplet $(0, 0, c_{\mathrm{mul}})$ as an encryption of 0 with respect to S'. □

Proposition 9 ($\mathbf{CPA}_2^D \not\Longrightarrow \mathbf{vCCA}_{\mathrm{SC}}$). *If there exists a CPA_2^D-secure scheme S, then there exists a scheme S' which is CPA_2^D-secure and $vCCA_{\mathrm{SC}}$-insecure.*

Proof. The proof is essentially identical to that of Proposition 5, but starting from a CPA_2^D-secure scheme S from which we create a scheme S' in a similar way. On one hand, the CPA_2^D-security of S' follows from that of S and the fact that a CPA_2^D adversary against S' cannot add $c^{\triangle}$ to the game state. On the other hand, the $\mathrm{vCCA}_{\mathrm{SC}}$-insecurity of S' follows from the fact that the $\mathrm{vCCA}_{\mathrm{SC}}$ game decryption oracle accepts $c^{\triangle}$ as it bears no relationship with the challenge ciphertext. □

4.3 Relations between $\mathbf{vCCA_{SC}}$ and $\mathbf{vCCA_{SC}^D}$ security

In this section, we establish the relationships between $\mathrm{vCCA}_{\mathrm{SC}}$ security (recall that only $\mathrm{vCCA}_{\mathrm{SC}}$ is studied in [20] and, as such, only denoted vCCA) and $\mathrm{vCCA}_{\mathrm{SC}}^D$ in both the correct regime and the general regime where approximate FHE are allowed. In a nutshell, we establish that, although the two notions are equivalent in the correct regime, $\mathrm{vCCA}_{\mathrm{SC}}^D$ security is strictly stronger than $\mathrm{vCCA}_{\mathrm{SC}}$ is the general case.

Lemma 10. *$vCCA_{SC}^D$ security implies $vCCA_{\mathrm{SC}}$ security.*

Proof. By definition of the two games, all decryption requests accepted by the $\mathrm{vCCA}_{\mathrm{SC}}$ decryption oracle are also accepted by the $\mathrm{vCCA}_{\mathrm{SC}}^D$ one (recall also Remark 3 on p. 12). It thus follows that any request performed by a $\mathrm{vCCA}_{\mathrm{SC}}$ adversary can also be performed by a $\mathrm{vCCA}_{\mathrm{SC}}^D$ one. □

Note that the above implication holds in the general regime i.e., independently of the correctness assumption.

We then prove a first result showing that $\mathrm{vCCA}_{\mathrm{SC}} \not\Longrightarrow \mathrm{vCCA}_{\mathrm{SC}}^D$ in the correct regime, under some condition on the probability that an adversary may bypass plaintext awareness.

Proposition 11. *Let S be a vCCA$_{\mathrm{SC}}$-secure scheme and let $\mu^{\perp}$ denotes the probability that $\mathsf{Dec}(u) = \perp$ for $u \xleftarrow{\$} \mathcal{C}$, then, under the correctness assumption, there exists an adversary against the vCCA$^{D}_{SC}$-security of S which achieves advantage $(1-\mu^{\perp})(1-1/|\mathcal{P}|)$.*

Proof. Consider a vCCA$_{\mathrm{SC}}$-secure scheme $S = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval})$ and assume $m_0^* = 0$, $m_1^* = 1$ and $c^* = \mathsf{Enc}(m_b^*)$. We now consider the following vCCA$^{D}_{\mathrm{SC}}$ attack against S. First, $\mathcal{A}$ picks a ciphertext c_{rnd} uniformly at random in $\mathcal{C}$. He or she then performs,

$$c_{\mathrm{mul}} = \mathsf{Eval}(\mathrm{mul}, c^*, c_{\mathrm{rnd}}).$$

where c_{mul} (as well as c_{rnd}) decrypts to $\perp$ with probability $\mu^{\perp}$[6]. Now, since it is a byproduct of the challenge ciphertext via an invocation of Eval, ciphertext c_{mul} is rejected by the vCCA$_{\mathrm{SC}}$ game decryption oracle. However, c_{mul} is accepted by the vCCA$^{D}_{\mathrm{SC}}$ game decryption oracle: since c_{rnd} cannot be part of the vCCA$^{D}_{\mathrm{SC}}$ game state (as $\mathcal{A}$ does not know the associated plaintext), then neither can be c_{mul}. When $\mathsf{Dec}(c_{\mathrm{mul}}) = 0$, then $\mathcal{A}$ decides that $b = 0$ and, under the correctness assumption, wins the vCCA$^{D}_{\mathrm{SC}}$ game with probability $1 - \frac{1}{|\mathcal{P}|}$. Hence the claim. □

Note that thanks to condition (2), this proposition can also easily be generalized to the general regime which also include approximate FHE schemes (in this case $\mathcal{A}$ decides that $b = 0$ when $\|\mathsf{Dec}(c_{\mathrm{mul}})\|_{\infty} \leq \varepsilon$ and wins the game with advantage $p_{\varepsilon}(1-\mu^{\perp})(1-1/|\mathcal{P}|)$). However this result is of limited interest as the above attack leads to a non-negligible advantage only if S is such that $1-\mu^{\perp} > \mathrm{neg}(\lambda)$. However, as already discussed in Sect. 3.2 (recall Remark 3, page 12 and its follow up discussion) all the vCCA$_{\mathrm{SC}}$-secure constructions proposed in [20] and revisited in Sect. 6 include the machinery necessary for their decryption *function* to return $\perp$ when given either an ill-formed ciphertext (which will then be the case of c_{rnd} with at least $1-\mathrm{neg}(\lambda)$ probability) or an evaluated ciphertext over non well-formed ones (which is then the case of c_{mul}). As a consequence, it is interesting to study the relationship between vCCA$_{\mathrm{SC}}$-security and vCCA$^{D}_{\mathrm{SC}}$-security *under the well-formedness assumption* whereby the adversary is limited to exploit only legit ciphertexts (well-formed fresh ciphertexts or ciphertexts derived from fresh well-formed ciphertexts via legit homomorphic evaluations).

Proposition 12. *Under both the FHE correctness and (the above) well-formedness assumptions, vCCA$_{\mathrm{SC}}$ security is equivalent to vCCA$^{D}_{SC}$ security.*

Proof. Following Lemma 10 we have that vCCA$^{D}_{\mathrm{SC}}$ security implies vCCA$_{\mathrm{SC}}$ security. For the other direction, we will now show that given a successful (passive) adversary $\mathcal{A}$ against the vCCA$^{D}_{\mathrm{SC}}$ security of a scheme S, there exists a successful (passive) adversary $\mathcal{B}$ against the vCCA$_{\mathrm{SC}}$ security of S which uses $\mathcal{A}$ as a subroutine. Then $\mathcal{A}$ can issue the following requests which $\mathcal{B}$ emulates as follows:

[6] Following the consistency assumption (4) (Sect. 2).

- When $\mathcal{A}$ issues a $\text{vCCA}^D_{\text{SC}}$ game encryption request for plaintext m, then $\mathcal{B}$ issues a vCCA_{SC} game encryption request to get ciphertext c which it returns to $\mathcal{A}$.
- When $\mathcal{A}$ issues the *unique* $\text{vCCA}^D_{\text{SC}}$ game challenge request for plaintexts m_0^*, m_1^* ($m_0^* \neq m_1^*$), then $\mathcal{B}$ issues a vCCA_{SC} game challenge request to get ciphertext c^* which it returns to $\mathcal{A}$. Additionally, $\mathcal{B}$ stores m_0^*, m_1^* as well as c^*.
- When $\mathcal{A}$ issues a $\text{vCCA}^D_{\text{SC}}$ game decryption request for *well-formed* (recall that $\mathcal{A}$ is passive) ciphertext c, then $\mathcal{B}$ runs the extractor over c to get

$$(f, c_1, ..., c_K) = \mathsf{Extract}(c),$$

and then proceeds as follows:
  - If $c^* \notin \{c_1, ..., c_K\}$, $\mathcal{B}$ simply issues a vCCA_{SC} game decryption request and forward the resulting plaintext (which is necessarily not $\perp$) to $\mathcal{A}$.
  - Otherwise (assuming wlog that the challenge ciphertext appears only once as the first position argument), $\mathcal{B}$ issues vCCA_{SC} game decryption requests for $c_2, ..., c_K$, getting plaintexts $m_2, ..., m_K$ which were the associated encryption function inputs (because of the correctness assumption). Then $\mathcal{B}$ compute $r_0 = f(m_0^*, m_2, ..., m_K)$ and $r_1 = f(m_1^*, m_2, ..., m_K)$ and returns r_0 when $r_0 = r_1$ (in this case, under the correctness assumption, $r_0 = r_1 = \mathsf{Dec}(c)$) and $\perp$ otherwise.

Thus, $\mathcal{B}$ can duly simulate all the $\text{vCCA}^D_{\text{SC}}$ game requests issued by $\mathcal{A}$. □

Note that this proof is performed under the passive adversary assumption under which all ciphertexts are well-formed. If we take a glimpse at the constructions that will be discussed in Sect. 6, this means that the SNARK proofs of correct homomorphic evaluations are always valid and that the associated extractor always exists. Thus, for the Designated-Verifier case, $\mathcal{B}$ does not need access to a verification oracle. Also, because this proof is done under the correctness assumption, $\mathsf{Extract}'$ (as defined in Sect. 3.2, Eq. (11)) is not needed for $\mathcal{B}$ to recover the encryption function inputs (as these can be recovered via calls to the decryption oracle of the vCCA_{SC} game that $\mathcal{B}$ is playing against).

In the general case, however, it turns out that the two notions can be separated as established by the following proposition.

Proposition 13 ($\text{vCCA}_{\text{SC}} \not\Longrightarrow \text{vCCA}^D_{\text{SC}}$). *In the general regime, if there exists a $vCCA^D_{SC}$-secure scheme S, then there exists a scheme S' which is $vCCA_{\text{SC}}$-secure but $vCCA^D_{SC}$-insecure, even against a passive adversary.*

Proof. We proceed similarly to the proof of Proposition 6 (and Proposition 8). Let us start from a $\text{vCCA}^D_{\text{SC}}$-secure scheme $S = (\mathsf{KeyGen}, \mathsf{EncDec}, \mathsf{Eval})$ from which we build the scheme S' with the only modification that

$$\mathsf{Enc}'(m) = \mathsf{Enc}(m + g(m)).$$

with function g as in the proof of Proposition 6.
S' is $vCCA_{\text{SC}}$-secure. Since S is $\text{vCCA}^D_{\text{SC}}$-secure, it is also vCCA_{SC}-secure (from

Lemma 10). Now, let $\mathcal{A}$ be a successful adversary against the vCCA_{SC} security of S'. It is then easy to build an adversary $\mathcal{B}$ against the vCCA_{SC} security of S. Indeed, $\mathcal{B}$ simulates $\mathcal{A}$ encryption and challenge requests simply by adding $g(m)$ to m. All other request are transferred "as is" by $\mathcal{B}$ to the vCCA_{SC} game against S.
S' is vCCA^D-insecure. Identical to proof of Proposition 6: the $\text{vCCA}^D_{\text{SC}}$ decryption oracle accepts the c_{mul} ciphertext as, recall (9) and (10), $\text{left}(c_{\text{mul}}) = \text{right}(c_{\text{mul}}) = 0$ (as c_{mul} is an encryption of 0 with respect to S').
Since this latter attack involves only legit ciphertexts, it can be performed by a passive adversary. □

Following Lemma 10 and Proposition 13 we can conclude that $\text{vCCA}^D_{\text{SC}}$ security is strictly stronger than vCCA_{SC} security in the general regime.

5 Relations among the multiple challenge notions

5.1 Relations between CPA^D_{SC} and CPA^D security

In this section, we first focus on CPA^D and study the relationship between the single and multiple-challenge variants of this notion. This is an interesting question as, unless the FHE scheme is restricted to the evaluation of univariate functions, the usual hybrid argument e.g. in [3] (theorem 4) for showing the equivalence (up to an increase in advantage linear in the number of challenge ciphertexts) between FTG-CPA[7] (resp. FTG-CCA) and LOR-CPA (resp. LOR-CCA) does not work directly. This is so because an adversary confronted to a hybrid game (where the encryption oracle replies according to $b = 0$ up to a random point after which it replies according to $b = 1$) can detect the transition between the first and second phase since ciphertexts from the two phases may interact via evaluation requests. The relationship between single and multiple-challenge variants of CPA^D was also explicitly left as an open question in [18].

Then, we also establish that, for CPA^D, the single and multiple challenge variants are (without surprise) equivalent in the correct regime and, more interestingly, that the two notions can be separated in the general regime (which is the non-trivial CPA^D setting).

We first recall the following well-known theorem from [3].

Theorem 14. *For any encryption scheme $S = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$, LOR-CPA is equivalent to FTG-CPA*[8].

[7] Recall that Find-Then-Guess (FTG) is the terminology for single challenge security notions in the foundational papers [3,4].

[8] More precisely [3] established that the advantage of a LOR-CPA (resp. LOR-CCA) adversary is bounded by $q_e \alpha_{\text{sc}}$, where q_e is an upper bound the number of encryption queries with $m_0 \neq m_1$ and α_{sc} is the advantage of an FTG-CPA (resp. FTG-CCA) adversary.

For CPA^D security, in the correct FHE regime, we have the following equivalence. This equivalence is not surprising since CPA^D security collapses onto CPA security for correct FHE.

Proposition 15. *For any correct FHE scheme, $S = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval})$, CPA^D security is equivalent to CPA$^D_{SC}$ security.*

Proof. For a correct FHE scheme, it is well-known that LOR-CPA^D is equivalent to LOR-CPA [18]. This means that an adversary to the LOR-CPA^D game has exactly the same advantage as an adversary to *the LOR-CPA^D game without the decryption oracle*, which is the same as the LOR-CPA game plus the evaluation oracle (recall that the LOR-CPA^D game decryption oracle, Sect. 3.1, takes indices from the game state rather than ciphertexts as input). Let's call this the LOR-CPA^E game ("CPA with an evaluation oracle"). It is easy to see that LOR-CPA^E is exactly LOR-CPA. For the same reasons, CPA$^D_{\mathrm{SC}}$ is equivalent to FTG-CPA. The claim then follows from theorem 14 above. □

In the general regime where approximate FHE are allowed, things are more interesting as we can actually separate the two notions. We start by proving the separation in the special case of additive FHE scheme.

Proposition 16. *In the general regime, if there exists an additive HE scheme S which is CPA^D-secure, then there exists an additive HE scheme S' which is CPA$^D_{SC}$-secure and CPA^D-insecure.*

Proof. So let us start with a CPA^D-secure *additive* HE scheme

$$S = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval}).$$

Then, consider the scheme $S' = (\mathsf{KeyGen}', \mathsf{Enc}', \mathsf{Dec}', \mathsf{Eval}')$ such that

$$\mathsf{Enc}'(m) = \mathsf{Enc}(m + g(m)),$$

where g is some non linear function such that $g(a+b) \neq g(a)+g(b)$[9]. Additionally KeyGen', Dec' and Eval' are the same as those of S.

S' is CPA$^D_{SC}$-secure. First of all, let us remark that the CPA$^D_1$ security of S' follows from the CPA^D security of S and the fact that the approximation noise $g(m)$ is independent of S secret key material (which is the only information not available to a CPA$^D_1$ adversary). So to break the CPA$^D_{\mathrm{SC}}$ security of S', an attacker has to exploit the challenge ciphertext. However, after the adversary issues his or her unique challenge request with $m_0 \neq m_1$ to get m_0^*, m_1^* and $c^* = \mathsf{Enc}'(m_b^*)$, he or she can only

- asks for a decryption of c^*, which is rejected by the CPA$^D_{\mathrm{SC}}$ decryption oracle since $m_0^* \neq m_1^*$,

[9] More precisely, we need g such that there exists a, b, a' and b' such that $a+b = a'+b'$ while $g(a) + g(b) \neq g(a') + g(b')$.

– asks for a decryption of $c_{\text{sum}} = \mathsf{Eval}'(\text{sum}, c^*, c^{(1)}, ..., c^{(K)})$ where[10] all the $c^{(i)}$'s are such that $m_0^{(i)} = m_1^{(i)}$. The decryption of c_{sum} is also blocked by the CPA_{SC}^D decryption oracle since

$$m_0^* + \sum_i m_0^{(i)} \neq m_1^* + \sum_i m_1^{(i)}.$$

So the adversary can learn nothing on b and the CPA_{SC}^D-security of S' follows.

S' is not CPA^D-secure. Now let the adversary issue two challenge requests with $m_0 \neq m_1$ getting,

$$m_0^*, m_1^*, c^* = \mathsf{Enc}'(m_b^*),$$

as well as

$$m_0^\dagger, m_1^\dagger, c^\dagger = \mathsf{Enc}'(m_b^\dagger),$$

such that $Z = m_0^* + m_0^\dagger = m_1^* + m_1^\dagger$ and $g(m_0^*) + g(m_0^\dagger) \neq g(m_1^*) + g(m_1^\dagger)$. The adversary then computes

$$c_{\text{sum}} = \mathsf{Eval}'(\text{sum}, c^*, c^\dagger)$$

which the CPA^D decryption oracle accepts since the left and right evaluations both give Z i.e., c_{sum} is an encryption of Z with respect to S'. However, with respect to S, c_{sum} is an encryption of $Z + g(m_b^*) + g(m_b^\dagger)$, hence the adversary gets $\mathsf{Dec}'(c_{\text{sum}}) = \mathsf{Dec}(c_{\text{sum}})$ such that

$$\|\mathsf{Dec}'(c_{\text{sum}}) - Z - g(m_b^*) - g(m_b^\dagger)\|_\infty \leq \varepsilon$$

as a result of a decryption request on c_{sum} (recall the definition of ε and p_ε in Eq. 2, p. 7). Since $g(m_b^*) + g(m_b^\dagger) \neq g(m_b^* + m_b^\dagger)$ and $g(m_0^*) + g(m_0^\dagger) \neq g(m_1^*) + g(m_1^\dagger)$ (and further assuming that $\|G_0 - G_1\|_\infty > 2\varepsilon$ with $G_b = g(m_b^*) + g(m_b^\dagger)$), the adversary recovers b with probability at least p_ε, leading the claim. □

To informally illustrate this (considering for simplicity sake $\mathcal{P} = \mathbb{Z}_t$, for some large *prime* plaintext modulus t), assuming $\varepsilon << 10000$ for the sake of an example, we can consider the following concrete setup, where $B = 10000$ and $g(x) = 2\varepsilon\lfloor x/B \rceil^2$ [11]. Then, as above, the adversary chooses $m_0^\star = m_0^\dagger = 10000$ as well as $m_1^\star = 0$ and $m_1^\dagger = 20000$. With these parameters, $Z = 20000$ and $\mathsf{Dec}'(c_{\text{sum}})$ belongs (with probability p_ε) to $[20000+3\varepsilon, 20000+5\varepsilon]$ when $b = 0$, or to $[20000+7\varepsilon, 20000+9\varepsilon]$ when $b = 1$.

We now further establish the separation result without the restriction to additive HE schemes.

[10] Under the assumption that $\forall m_0^*, m_1^* \in \mathcal{P}$ such that $m_0^* \neq m_1^*$ and $\forall k \in \mathbb{N}^*$ we have $k * m_0^* \neq k * m_1^*$, we can assume, without loss of generality that c^* appears only once and in the first place in the $\mathsf{Eval}'(\text{sum}, ...)$ arguments. Note that this requirement can easily be satisfied by $\mathcal{P}$ being a field.

[11] Stricto sensu, to ensure the boundedness of $g(x)$, it would be preferable to choose $g(x) = 2\varepsilon \min\left(L, \lfloor x/B \rceil^2\right)$ with e.g. $L = 5$ for our example to work. That way, S' is also an approximate FHE scheme consistent with our definition (2) (p. 7).

Corollary 17 ($\mathbf{CPA}^D_{\mathbf{SC}} \not\Longrightarrow \mathbf{CPA}^D$). *In the general regime, if there exists an FHE scheme S which is CPA^D-secure, then there exists an FHE scheme S' which is CPA^D_{SC}-secure and CPA^D-insecure.*

Proof. So let us start with a CPA^D-secure FHE scheme

$$S = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Add}, \mathsf{Mul}).$$

Then, consider the scheme $S' = (\mathsf{KeyGen}', \mathsf{Enc}', \mathsf{Dec}', \mathsf{Add}', \mathsf{Mul}')$ such that

$$\mathsf{Enc}'(m) = (\mathsf{Enc}(m), \mathsf{Enc}(g(m))) = (c_0, c_1) = c,$$

(with g being the same as in the proof of the previous Proposition 16) and

$$\mathsf{Dec}'(c) = \mathsf{Dec}(c_0) + \mathsf{Dec}(c_1).$$

Now we consider the following homomorphic addition and multiplication operators:

$$\mathsf{Add}'(c, c') = (\mathsf{Add}(c_0, c'_0), \mathsf{Add}(c_1, c'_1))$$

and

$$\mathsf{Mul}'(c, c') = (\mathsf{Mul}(c_0, c'_0), \mathsf{Enc}(0)).$$

Essentially, in S', the approximation noise is encrypted separately to the message (to make both easily separable) and the multiplication operator resets that noise. So as soon as the adversary performs a multiplication, he or she closes the information channel that function g opens. Although S' is duly fully homomorphic, we therefore end up in the same conditions as in the proof of Proposition 16. Indeed, in any successful $\mathrm{CPA}^D_{\mathrm{SC}}$ or CPA^D attack involving both homomorphic additions and multiplications, the multiplications are redundant. □

Since CPA^D security trivially implies $\mathrm{CPA}^D_{\mathrm{SC}}$ security, the following result is a direct consequence of Corollary 17.

Proposition 18. *In the general regime, CPA^D is strictly stronger than CPA^D_{SC}.*

Note that the above proposition (partly) settles the question of the relationship between single and multiple-challenge CPA^D security that was left open in [18] (p. 14): "It remains an interesting open question to find out the relationship between $(q;\ell)$-IND-CPA^D and $(q;\ell+1)$-IND-CPA^D securities (and same for SIM-CPA^D)." (in their notations, ℓ is the number of queries to the encryption oracle with $m_0 \neq m_1$ and q the number of decryption queries). Indeed, we have shown above that, even for $q = 1$, there exists homomorphic schemes which are $(q;1)$-CPA^D-secure while being $(q,2)$-CPA^D-insecure (in the notations of [18]). Of course, to completely settle the above question we also need to prove separation or equivalence of (q,ℓ)-CPA^D-security and $(q,\ell+1)$-CPA^D-security with $\ell > 2$. We leave this remaining question as an open problem.

5.2 Relations between vCCA$_{\mathbf{SC}}$ and vCCA security

Recall that [20] defines and studies only vCCA$_{\mathrm{SC}}$ security (also recall that in that paper it is simply referred to as vCCA). The question of the relationship between vCCA$_{\mathrm{SC}}$ security and LOR-vCCA security (or simply vCCA security with our present conventions) therefore deserves to be settled. So let LOR-vCCA denote the multiple challenges variant of vCCA in which the decryption oracle condition (7) is replaced by

$$C^* \cap \{c_1, ..., c_K\} \neq \varnothing, \tag{13}$$

where C^* is the set of challenge ciphertexts. We then have the proposition below.

Proposition 19. *vCCA security is equivalent to vCCA$_{\mathrm{SC}}$ security.*

Proof. The standard hybrid argument, e.g. in the proof of [3, Theorem 4] (which corresponds to Theorem 14 for both CPA and CCA), holds without modification, since an adversary confronted to a hybrid game (where the encryption oracle replies according to $b = 0$, up to a random point after which it replies according to $b = 1$) *cannot* detect the transition between the first and second phases. Indeed, although challenge ciphertexts from both phases may interact via homomorphic evaluations, condition (13) above guarantees that such interactions lead to ciphertexts rejected by the above LOR-vCCA decryption oracle. □

Note that in the above proof, we make no assumption about the correctness of the FHE scheme, so the above equivalence holds in the general regime.

As a consequence of Proposition 13, this establishes that the single challenge variant of vCCA^D security, vCCA$^D_{\mathrm{SC}}$, is already strictly stronger than the multiple challenge variant of vCCA.

5.3 Relations between vCCA$^{\boldsymbol{D}}_{\mathbf{SC}}$ and vCCA$^{\boldsymbol{D}}$ security

Lastly, we now unveil the relationship between the single and multiple challenge variant of vCCA^D security. Similarly to the CPA^D case, there is a distinction between the correct and general regime.

Proposition 20. *In the correct regime, vCCA^D is equivalent to vCCA$^D_{SC}$.*

Proof. The claim follows directly from proposition 12 (and its straightforward generalization to the multiple challenges variants of vCCA and vCCA^D) as well as proposition 19 above. □

We now turn to the general regime and, as in Sect. 5.1, first consider the case of linearly homomorphic schemes.

Proposition 21. *In the general regime, if there exists an additive HE scheme S which is vCCA^D-secure, then there exists an additive HE scheme S' which is vCCA$^D_{SC}$-secure and vCCA^D-insecure.*

Proof. We proceed similarly to the proof of Proposition 16. So let us start with a vCCA^D-secure *additive* HE scheme $S = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval})$ from which we build the scheme S' with the only modification that

$$\mathsf{Enc}'(m) = \mathsf{Enc}(m + g(m)),$$

where g is as in the proof of Proposition 16.

S' is $vCCA^D_{SC}$-secure. Since vCCA^D security trivially implies $\text{vCCA}^D_{\text{SC}}$ security, S is $\text{vCCA}^D_{\text{SC}}$-secure. Let $\mathcal{A}$ be a successful adversary against the $\text{vCCA}^D_{\text{SC}}$ security of S'. It is then easy to build an adversary $\mathcal{B}$ against the $\text{vCCA}^D_{\text{SC}}$ security of S. Indeed, $\mathcal{B}$ simulates $\mathcal{A}$ encryption and challenge requests simply by adding $g(m)$ to m. All other request are transferred "as is" by $\mathcal{B}$ to the $\text{vCCA}^D_{\text{SC}}$ game against S.

S' is $vCCA^D$-insecure. Identical to proof of Proposition 16: the vCCA^D decryption oracle accepts the c_{sum} ciphertext as, recall (9) and (10), $\text{left}(c_{\text{sum}}) = \text{right}(c_{\text{sum}}) = Z$ (as an encryption of Z with respect to S'). □

Corollary 22 ($\mathbf{vCCA^D_{SC} \not\Rightarrow vCCA^D}$). *In the general regime, if there exists an FHE scheme S which is $vCCA^D$-secure, then there exists an FHE scheme S' which is $vCCA^D_{SC}$-secure and $vCCA^D$-insecure.*

Proof. Identical to that of Corollary 17. □

Since vCCA^D security trivially implies $\text{vCCA}^D_{\text{SC}}$ security, the following result is a direct consequence of Corollary 22.

Proposition 23. *In the general regime, $vCCA^D$ is strictly stronger than $vCCA^D_{SC}$.*

It follows that vCCA^D security is the strongest CCA security notion so far known to be achievable by FHE in the general regime.

6 Construction blueprints

In this section, we revisit the four construction blueprints proposed in [20] to leverage CPA-secure and correct FHE schemes into vCCA_{SC}-secure schemes, and study both their applicability in the general regime where approximate FHE are allowed as well as their vCCA^D security. As such, we emphasize that the constructions themselves are not new.

6.1 Private key constructions

We first consider the Encrypt-then-Sign construction blueprint proposed in [20]. The construction is built over a public-key FHE scheme $\mathcal{E}_H$, a public-key signature scheme $\Sigma = (\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$, as well as a (publicly verifiable or designated-verifier) SNARK, $\Pi = (\mathsf{Setup}, \mathsf{Prove}, \mathsf{Verify})$, for langage

$$L_1 = \left\{ c_e | \exists f \in \mathcal{F}_H, \exists (c_1, \pi_1), ..., (c_K, \pi_K) \in \mathcal{C}^K, \begin{array}{l} \Sigma.\mathsf{Verify}(\Sigma.\mathsf{pk}, c_i, \pi_i), \forall i \\ c_e = \mathcal{E}_H.\mathsf{Eval}(\mathcal{E}_H.\mathsf{pk}, f, c_1, ..., c_K) \end{array} \right\},$$

to obtain an encryption scheme $\mathcal{E}^\star_H$ defined as follows:

- $\mathcal{E}_H^\star$.KeyGen: run $\mathcal{E}_H$.KeyGen, Σ.KeyGen, Π.Setup, let $\mathsf{ek} = (\mathcal{E}_H.\mathsf{pk}, \Sigma.\mathsf{sk})$ as well as $\mathsf{sk} = (\mathcal{E}_H.\mathsf{sk}, \Sigma.\mathsf{pk}, [\Pi.\mathsf{vk}])$.
- $\mathcal{E}_H^\star$.Enc: given $m \in \mathcal{P}$ generate ciphertext

$$(c, \pi) = (\mathcal{E}_H.\mathsf{Enc}(\mathcal{E}_H.\mathsf{pk}, m), \Sigma.\mathsf{Sign}(\Sigma.\mathsf{sk}, c)).$$

- $\mathcal{E}_H^\star$.Eval: given ciphertexts $(c_1, \pi_1), ..., (c_K, \pi_K)$ such that $\Sigma.\mathsf{Verify}(c_i, \pi_i), \forall i$, generate ciphertext (c_e, π_e) such that

$$c_e = \mathcal{E}_H.\mathsf{Eval}(\mathcal{E}_H.\mathsf{pk}, f, c_1, ..., c_K),$$

  and

$$\pi_e = \Pi.\mathsf{Prove}(c_e, (f, (c_1, \pi_1), ..., (c_K, \pi_K))).$$

- $\mathcal{E}_H^\star$.Dec: given ciphertext (c, π) return $\mathcal{E}_H.\mathsf{Dec}(\mathcal{E}_H.\mathsf{sk}, c)$ when $\Sigma.\mathsf{Verify}(\Sigma.\mathsf{pk}, c, \pi) = \mathsf{True}$ or $\Pi.\mathsf{Verify}([\Pi.\mathsf{vk}], c, \pi) = \mathsf{True}$, and $\perp$ otherwise.

Intuitively, the essence of this construction is to rely on a trusted encryption oracle that generates only well-formed ciphertexts with respect to $\mathcal{E}_H$ and signs them such that they are recognizable. As such, this construction is not public key, due to the presence of $\Sigma.\mathsf{sk}$ in ek. Also, let us emphasize that this construction satisfies the compactness property which is implicitly assumed for FHE as the size of the output of Eval is independent of the size of f and, in particular, of its arity, thanks to the succinctness of the SNARK. To improve the practicality of this construction (at the expense of input privacy and compactness), it is also possible to modify it such that the statements for which the Π outputs a proof during Eval does not have to include the verification of the input ciphertexts' signatures. In that case, both the input *and* output ciphertexts must be available to the decryption algorithm which is then responsible for verifying the signatures of the former. When this is the case, Π is for the simpler language

$$L_2 = \{c_e, c_1, ..., c_K | \exists f \in \mathcal{F}_H, c_e = \mathcal{E}_H.\mathsf{Eval}(\mathcal{E}_H.\mathsf{pk}, f, c_1, ..., c_K)\}, \tag{14}$$

and Eval and Dec are modified as follows:

- $\mathcal{E}_H^\star$.Eval: given ciphertexts $(c_1, \pi_1), ..., (c_K, \pi_K)$ compute

$$(c_e = \mathcal{E}_H.\mathsf{Eval}(\mathcal{E}_H.\mathsf{pk}, f, c_1, ..., c_K), \pi_e = \Pi.\mathsf{Prove}((c_e, c_1, ..., c_K), f)).$$

  and return ciphertext $((c_e, \pi_e), (c_1, \pi_1), ..., (c_K, \pi_K))$.
- $\mathcal{E}_H^\star$.Dec (fresh ciphertext): given (c, π), if $\Sigma.\mathsf{Verify}(\Sigma.\mathsf{pk}, c, \pi) = \mathsf{True}$ return $\mathcal{E}_H.\mathsf{Dec}(\mathcal{E}_H.\mathsf{sk}, c)$, and return $\perp$ otherwise.
- $\mathcal{E}_H^\star$.Dec (evaluated ciphertext): given $((c_e, \pi_e), (c_1, \pi_1), ..., (c_K, \pi_K))$ return $\mathcal{E}_H.\mathsf{Dec}(\mathcal{E}_H.\mathsf{sk}, c_e)$ when $\Pi.\mathsf{Verify}([\Pi.\mathsf{vk}], c_e, \pi_e) = \mathsf{True}$ and $\Sigma.\mathsf{Verify}(\Sigma.\mathsf{pk}, c_i, \pi_i) = \mathsf{True}, \forall i$ and $\perp$ otherwise.

In this modified construction, the signature scheme can be replaced by a MAC $M = (\mathsf{KeyGen}, \mathsf{Tag}, \mathsf{Verify})$, leading to the Encrypt-then-MAC blueprint of [20].

The above Encrypt-then-Sign construction was proved in [20] to lead a vCCA_{SC}-secure scheme from a CPA-secure *correct* FHE scheme, a SUF-CMA-secure signature scheme and a simulation-sound extractable SNARK (which implies the existence of an extractor as defined in Sect. 3.2). Their proof technique consists in showing that a successful vCCA_{SC} attack over scheme $\mathcal{E}_H^\star$ implies a successful CCA2 attack against the *private key* (non homorphic) encryption scheme obtained by associating $\mathcal{E}_H$ and Σ. It turns out that the security of this construction goes beyond this setting as we now prove that the above Encrypt-then-Sign blueprint in fact offers vCCA^D security beyond the correct FHE regime, as long as we instantiate it from a CPA^D-secure rather than CPA-secure/correct FHE.

To do so, we now prove that an adversary breaking vCCA^D security on the above construction also breaks the CPA^D security of the underlying FHE scheme, thus leading to a contradiction with the the CPA^D security of the latter.

Proposition 24. *Let $\mathcal{A}$ be an adversary against the vCCA^D security of $\mathcal{E}_H^\star$, then, under the assumption that Σ is SUF-CMA secure and Π is straightline-extractable, there exists an adversary $\mathcal{B}$ against the CPA^D security of $\mathcal{E}_H$ which uses $\mathcal{A}$ as a subroutine.*

Proof. We thus start with the vCCA^D security game between an adversary $\mathcal{A}$ and the challenger. In a first step, we can replace all the verifications of the signatures by checking whether the signatures have been generated by the challenger. If this is not the case, the signature is refused: this can only make a difference if the adversary can forge a new valid signature, which breaks the SUF-CMA security of the signature. This happens with negligible probability only. In a second step, we can replace all the verifications of the SNARKs by invoking the verification oracle and by additionally checking the extracted witnesses: this can only make a difference if the extracted witness is invalid, while the proof is accepted, which should happen with negligible probability from the knowledge soundness.

We are now in the last game, where we build an adversary $\mathcal{B}$ against the CPA^D security, from the adversary $\mathcal{A}$: $\mathcal{B}$ initially runs $\Pi.\mathsf{Setup}$ and $\Sigma.\mathsf{KeyGen}$ and communicates the associated public material to $\mathcal{A}$. Additionally, $\mathcal{B}$ mimics the CPA^D game state and initially starts with an empty state $S^{\mathcal{B}} = []$. Then, given a ciphertext c, we denote by $\mathsf{idx}(c)$, its index in the game state $S^{\mathcal{B}}$ (which is the same as the index at which the ciphertext is stored in the CPA^D game state S). Then $\mathcal{A}$ can issue the following requests, which $\mathcal{B}$ emulates as follows:

- When $\mathcal{A}$ issues a vCCA^D game encryption request for plaintext m, then $\mathcal{B}$ issues a CPA^D game encryption request to get ciphertext c. He or she then does $S^{\mathcal{B}} := [S^{\mathcal{B}}; (m, m, c)]$, generates $\pi = \Sigma.\mathsf{Sign}(\Sigma.\mathsf{sk}, c)$ and return (c, π) to $\mathcal{A}$.
- When $\mathcal{A}$ issues a vCCA^D game challenge request for plaintexts m_0, m_1 ($m_0 \neq m_1$), then $\mathcal{B}$ issues a CPA^D game challenge request to get ciphertext c. He or she then does $S^{\mathcal{B}} := [S^{\mathcal{B}}; (m_0, m_1, c)]$, generates $\pi = \Sigma.\mathsf{Sign}(\Sigma.\mathsf{sk}, c)$ and return (c, π) to $\mathcal{A}$.

– When $\mathcal{A}$ issues a vCCA^D game decryption request for ciphertext (c, π), $\mathcal{B}$ proceeds as follows:
  - If $\Sigma.\mathsf{Verify}(\Sigma.\mathsf{pk}, c, \pi) = \mathsf{True}$ (i.e., when (c, π) is a fresh well-formed ciphertext) he or she issues a CPA^D game decryption request on $\mathsf{idx}(c)$ and return the result to $\mathcal{A}$.
  - If $\Pi.\mathsf{Verify}([\Pi.\mathsf{vk}], c, \pi) = \mathsf{True}$, $\mathcal{B}$ invokes Π's $\mathsf{Extract}$ procedure over $(c; \pi)$ to get $f; (c_1; \pi_1), ..., (c_K; \pi_K)$. In this case, if $\Sigma.\mathsf{Verify}(\Sigma.\mathsf{pk}, c_i, \pi_i)) = \mathsf{False}$ for some i he or she returns $\perp$ to $\mathcal{A}$. Otherwise (when (c, π) is a well-formed evaluated ciphertext), he or she then does a CPA^D game evaluation request with parameters $f; \mathsf{idx}(c_1), ..., \mathsf{idx}(c_K)$ and get ciphertext $c' = c$ (recall that Eval is deterministic) in return (with also the effect of adding $c' = c$ along with the associated left and right cleartext evaluations in the CPA^D game state), he or she also performs the left and right cleartext evaluations for his or herself to get
$$m'_0 = f(S^{\mathcal{B}}[\mathsf{idx}(c_1)].m_0, ..., S^{\mathcal{B}}[\mathsf{idx}(c_K)].m_0)$$
and
$$m'_1 = f(S^{\mathcal{B}}[\mathsf{idx}(c_1)].m_1, ..., S^{\mathcal{B}}[\mathsf{idx}(c_K)].m_1)$$
and do $S^{\mathcal{B}} := [S^{\mathcal{B}}; (m'_0, m'_1, c')]$. Finally, $\mathcal{B}$ issues a CPA^D game decryption request with $\mathsf{idx}(c') = |S^{\mathcal{B}}|$ and returns the result to $\mathcal{A}$.
  - Otherwise, $\mathcal{B}$ returns $\perp$ to $\mathcal{A}$.

Thus, $\mathcal{B}$ can duly simulate all the vCCA^D game requests issued by $\mathcal{A}$. And eventually, $\mathcal{B}$ forwards the decision of $\mathcal{A}$: when $\mathcal{A}$ wins, $\mathcal{B}$ wins. □

6.2 Public-key constructions

We now consider the public key, designated-verifier[12] construction blueprint proposed in [20] which we refer to as the *CCA2-Companion-Ciphertext* approach in this paper. The construction is built over a public-key FHE scheme $\mathcal{E}_H$, a public-key (CCA2-secure) scheme $\mathcal{E} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$, and a publicly verifiable or designated verifier SNARK $\Pi = (\mathsf{Setup}, \mathsf{Prove}, \mathsf{Verify})$ for langage (14), to obtain encryption scheme $\mathcal{E}^\star_H$:

– $\mathcal{E}^\star_H.\mathsf{KeyGen}$: run $\mathcal{E}_H.\mathsf{KeyGen}$, $\mathcal{E}.\mathsf{KeyGen}$, $\Pi.\mathsf{Setup}$, let $\mathsf{ek} = (\mathcal{E}_H.\mathsf{pk}, \mathcal{E}.\mathsf{pk})$ as well as $\mathsf{sk} = (\mathcal{E}_H.\mathsf{sk}, \mathcal{E}.\mathsf{sk}, [\Pi.\mathsf{vk}])$.
– $\mathcal{E}^\star_H.\mathsf{Enc}$: given $m \in \mathcal{P}$ generate ciphertext, with $|$ denoting the concatenation operator, $(c, c') = (\mathcal{E}_H.\mathsf{Enc}(\mathcal{E}_H.\mathsf{pk}, m; r), \mathcal{E}.\mathsf{Enc}(\mathcal{E}.\mathsf{pk}, m|r))$.
– $\mathcal{E}^\star_H.\mathsf{Eval}$: given ciphertexts $(c_1, c'_1), ..., (c_K, c'_K)$, compute
$$(c_e = \mathcal{E}_H.\mathsf{Eval}(\mathcal{E}_H.\mathsf{pk}, f, c_1, ..., c_K), \pi_e = \Pi.\mathsf{Prove}((c_e, c_1, ..., c_K), f)).$$
and return ciphertext $((c_e, \pi_e), (c_1, c'_1), ..., (c_K, c'_K))$.

[12] In [20] terminology this just tells whether or not the well-formedness of fresh ciphertexts is verifiable publicly or privately. This is independent of whether the SNARK is publicly verifiable or designated-verifier.

- $\mathcal{E}^{\star}_H.\mathsf{Dec}$ (fresh ciphertext): given (c, c'), if $\mathsf{Verif}(\mathcal{E}.\mathsf{sk}, c, c') = \mathsf{True}$ then return $\mathcal{E}_H.\mathsf{Dec}(\mathcal{E}_H.\mathsf{sk}, c)$, and return $\perp$ otherwise[13].
- $\mathcal{E}^{\star}_H.\mathsf{Dec}$ (evaluated ciphertext): given ciphertext $((c_e, \pi_e), (c_1, c'_1), ..., (c_K, c'_K))$, if $\mathsf{Verif}(\mathcal{E}.\mathsf{sk}, c_i, c'_i) = \mathsf{True}$, $\forall i$ and $\Pi.\mathsf{Verify}([\Pi.\mathsf{vk}], c_e, \pi_e)$, return $\mathcal{E}_H.\mathsf{Dec}(\mathcal{E}_H.\mathsf{sk}, c_e)$. Return $\perp$ otherwise.

Where $\mathsf{Verif}(\mathcal{E}.\mathsf{sk}, c, c')$ runs $(m', r') = \mathcal{E}.\mathsf{Dec}(\mathcal{E}.sk, c')$ and returns True iff

$$c = \mathcal{E}_H.\mathsf{Enc}(\mathcal{E}_H.\mathsf{pk}, m'; r').$$

Intuitively, the essence of this construction is to define fresh ciphertexts as the association of an FHE ciphertext encrypting m by means of randomness r and another ciphertext encrypting the concatenation of m and r under a CCA2-secure encryption scheme. This allows to verify the well-formedness of these fresh ciphertexts by first decrypting the companion CCA2 ciphertext to recover m and r[14] and then checking that the associated FHE ciphertext is indeed equal to $\mathcal{E}_H.\mathsf{Enc}(\mathcal{E}_H.\mathsf{pk}, m; r)$ (note that the verification may succeed when $\mathcal{E}_H.\mathsf{Dec}(\mathcal{E}_H.\mathsf{sk}, \mathcal{E}_H.\mathsf{Enc}(\mathcal{E}_H.\mathsf{pk}, m; r)) \neq m$ which is what we want when the correctness assumption does not hold for $\mathcal{E}_H$). The approach, however, has the drawback that it cannot achieve any form of input privacy as this verification requires the knowledge of the CCA2 scheme decryption key and, as a consequence, can be performed only in the decryption function of the overall scheme, requiring the availability of the input ciphertexts. This also makes it non compact.

The above CCA2-Companion-Ciphertext blueprint was proved in [20] to lead a vCCA_{SC}-secure scheme from a CPA-secure *correct* FHE scheme, a CCA2-secure scheme and a simulation-sound extractable SNARK (which implies the existence of an extractor as defined in Sect. 3.2). Their proof technique consists in showing that a successful vCCA_{SC} attack over scheme $\mathcal{E}^{\star}_H$ implies a successful CCA2 attack on the companion CCA2 scheme. As in the previous section, it turns out that the security of this construction goes beyond this setting as we now prove that it also achieves vCCA^D security in the general regime, as long as we instantiate it from a CPA^D-secure rather than CPA-secure/correct FHE.

Proposition 25. *Let $\mathcal{A}$ be an adversary against the vCCA^D security of $\mathcal{E}^{\star}_H$, then, under the assumption that $\mathcal{E}$ is CCA2-secure and Π is straightline-extractable, there exists an adversary $\mathcal{B}$ against the CPA^D security of $\mathcal{E}_H$ which uses $\mathcal{A}$ as a subroutine.*

[13] Here, we slightly depart from the construction of [20] in the following sense. When decrypting a fresh ciphertext (c, c'), they indeed proceed by calling $\mathcal{E}.\mathsf{Dec}(\mathcal{E}.\mathsf{sk}, c')$ to get m and r and return m when $\mathsf{Verif}(\mathcal{E}.\mathsf{sk}, c, c') = \mathsf{True}$ (i.e., they never decrypt the FHE ciphertext). We, on the contrary, return $\mathcal{E}_H.\mathsf{Dec}(\mathcal{E}_H.\mathsf{sk}, c)$ when $\mathsf{Verif}(\mathcal{E}.\mathsf{sk}, c, c') = \mathsf{True}$. Although both options are equivalent under the correctness assumption of $\mathcal{E}_H$, this is not the case in the general regime. However, when $\mathcal{E}_H$ is CPA^D-secure (as required for the construction in the general regime), this difference has no security implications.

[14] As such, in the CCA2-Companion-Ciphertext construct, we exactly get the additional extractor $\mathsf{Extract}'$ needed in the vCCA^D game definition in the public key case (Sect. 3.3).

Proof. The proof is quite similar to that of Proposition 24 except that we slightly modify the CPA^D encryption oracle (but *not* the challenge oracle) such that it further takes randomness r as a parameter (this is benign for public-key FHE schemes, and all FHE schemes in this paper are public key). Also, $\mathcal{B}$ initially runs $\Pi.\mathsf{Setup}$ and $\mathcal{E}.\mathsf{KeyGen}$ and communicate the associated public material to $\mathcal{A}$. When $\mathcal{B}$ receives a challenge request with $m_0 \neq m_1$, it forwards it to the CPA^D challenger to get $c = \mathcal{E}_H.\mathsf{Enc}(\mathcal{E}_H.\mathsf{pk}, m_b; r)$ with unknown b and r, he or she then updates $S^{\mathcal{B}} := [S^{\mathcal{B}}; (m_0, m_1, c)]$ and returns $(c, \mathcal{E}.\mathsf{Enc}(\mathcal{E}.\mathsf{pk}, m_0 || r'))$ for some randomly chosen r' (note that from the CCA2 security of $\mathcal{E}$, $\mathcal{A}$ cannot distinguish between $\mathcal{E}.\mathsf{Enc}(\mathcal{E}.\mathsf{pk}, m_0 || r')$ and $\mathcal{E}.\mathsf{Enc}(\mathcal{E}.\mathsf{pk}, m_b || r)$). When $\mathcal{B}$ processes a decryption request (assuming evaluated ciphertexts), $\mathcal{B}$ retrieves the input ciphertexts using $\mathsf{Extract}$. The input ciphertexts which are challenge ones are already in his or her internal state (ditto for the CPA^D defender). For the input ciphertexts which are challenge-independent, the message and randomness are recovered by $\mathcal{B}$ via the decryption of the CCA2 companion ciphertexts (which thus implements the $\mathsf{Extract}'$ defined in Sect. 3.3). Then $\mathcal{B}$ can issue the proper CPA^D encryption requests (with the additional randomness parameter) to populate the CPA^D defender state (and his or her mirrored one at the same time). Then $\mathcal{B}$ can issue the CPA^D evaluation request with the appropriate game state indices to obtain $c' = c$ (due to the deterministic evaluation assumption) and add it to the CPA^D defender game state. Finally, $\mathcal{B}$ issues the CPA^D decryption request with $\mathsf{idx}(c)$. □

Lastly, let us emphasize that the (compact) Naor-Yung-based [21] construct of [20], which, in order to encrypt a plaintext, associates two FHE ciphertexts of this plaintext under different keys, and bind them by a proof that these two ciphertexts are encrypting the same plaintext, requires *perfect* correctness. Indeed, in [21] (definition 3.4), the scheme used in the construction must verify $\forall m \in \mathcal{P}, \forall r \in \{0;1\}^{p(n)}, \mathsf{Dec}(\mathsf{Enc}(m, r)) = m$, and this strong property lies at the heart of the validity of the proof in [21], see also [11]. As such it is not applicable in the general case where approximate FHE schemes are allowed.

Still, vCCA^D-secure constructions achieving compactness in the public-key setting can be obtained by replacing the CCA2-companion ciphertext (which essentially provides a designated verifier proof of plaintext awareness) by a *publicly verifiable* zk–SNARK Π_0 for language

$$L_3 = \{c | \exists m \in \mathcal{P}, \exists r \in \mathsf{COIN}, c = \mathcal{E}_H.\mathsf{Enc}(\mathcal{E}_H.\mathsf{pk}, m; r)\}.$$

This leads to a construction blueprint which is *identical* to the first Encrypt-then-Sign blueprint in previous Sect. 6.1, but with the signature scheme Σ replaced by Π_0 and the SNARK Π replaced by a SNARK Π_1 (which can be either publicly verifiable or designated verifier) for the following language

$$L_4 = \left\{ c_e | \exists f \in \mathcal{F}_H, \exists (c_1, \pi_1), ..., (c_K, \pi_K) \in \mathcal{C}^K, \begin{array}{l} \Pi_0.\mathsf{Verify}(c_i, \pi_i), \forall i \\ c_e = \mathcal{E}_H.\mathsf{Eval}(\mathcal{E}_H.\mathsf{pk}, f, c_1, ..., c_K) \end{array} \right\}.$$

Π_0 has to be publicly verifiable since Π_1's proofs are generated by the adversary which cannot be granted access to a private verification key for Π_0. To prove

the vCCA^D security of this later construct (under the assumption that both Π_0 and Π_1 are straightline extractable) we proceed exactly as in the proof of Proposition 25, with $\mathcal{B}$ operating both Π_0 and Π_1. The main difference is that we construct an adversary $\mathcal{B}$ against the CPA^D security of scheme $\mathcal{E}'_H$ (rather than $\mathcal{E}_H$) which is obtained from scheme $\mathcal{E}_H$ by just modifying the encryption function such that it also generates a proof of well-formedness i.e.,

$$(c, \pi) = \mathcal{E}'_H.\mathsf{Enc}(\mathcal{E}_H.\mathsf{pk}, m; r) = (\mathcal{E}_H.\mathsf{Enc}(\mathcal{E}_H.\mathsf{pk}, m; r), \Pi_0.\mathsf{Prove}(c, (m, r))).$$

In particular, upon decrypting a fresh ciphertext, $\mathcal{E}'_H$ decryption function ignores any proof material and for evaluated ciphertexts decryption no proof material is expected. Because Π_0 is zero knowledge, $\mathcal{E}'_H$ trivially inherits its CPA^D security from that of $\mathcal{E}_H$. Then challenge and decryption requests are processed as in the proof of Prop. 25 with the following slight differences:

- When $\mathcal{B}$ receives a challenge request with $m_0 \neq m_1$, it forwards it to the CPA^D challenger to get $(c, \pi) = (\mathcal{E}_H.\mathsf{Enc}(\mathcal{E}_H.\mathsf{pk}, m_b; r), \Pi_0.\mathsf{Prove}(c, (m_b, r)))$, updates its internal state $S^{\mathcal{B}} := [S^{\mathcal{B}}; (m_0, m_1, c)]$ and returns (c, π) to $\mathcal{A}$.
- $\mathsf{Extract}'$ (required in the simulation of $\mathcal{A}$'s decryption requests) is realized by means of Π_0 extractor which $\mathcal{B}$ can invoke.

Note that $\mathcal{B}$ only has access to the traces of execution of $\mathcal{A}$ (which forms the auxiliary data of Π_0's extractor), therefore $\mathsf{Extract}'$ is not defined for proofs generated by the CPA^D defender (and thus $\mathcal{B}$ cannot retrieve b by that mean).

7 Conclusion and future work

Following the work of Manulis & Nguyen [20] as well as the improvements on that work we presented in this paper, designing practical FHE-style malleable schemes enforcing CCA security properties beyond the CCA1 barrier seems within reach, at least for specific applications. Indeed, recent advances in SNARK for ring arithmetic, such as [13], give us the necessary toolbox for attempting concrete instantiations of the construction blueprints discussed in Sect. 6. Furthermore, in many usual applications of FHE, the set of algorithms that needs to run in the encrypted domain is very limited (for example, a FHE aggregation server involved in a Federated Training protocol for a machine learning model may only have to run a simple average [14] or a majority voting algorithm [15,16]). This gives us hope to be able to design practical vCCA^D-secure schemes with simplified SNARK or Verifiable Computing techniques tailored to these sets of algorithms. Lastly, it will also be interesting to investigate which building blocks are friendly towards each others e.g., finding "SNARK friendly" signature schemes for concrete instantiation of the Encrypt-then-Sign blueprint.

Also, following a recent burst of new CPA^D attacks on both noise-flooded CKKS and "exact" schemes such as BFV, BGV or TFHE [17,7,8] new FHE security paradigms are being proposed. As an example, Alexandru et al. [1] have proposed a new *weaker* variant of CPA^D security, termed application-aware

security. In essence, this new definition acknowledges that for non-exact FHE schemes, CPA^D security should be defined relatively to a function class $\mathcal{F}_C$ and a ciphertext noise estimation strategy, rather than absolutely. With respect to that new security notion, the cryptosystem parameters should then be set relatively to these, and the homomorphic evaluations should be limited to the functions or circuits in the class. However, one of the main drawbacks of the application-aware approach is that the burden of enforcing the above constraints lies, so far, solely on the library user's shoulders (see also [2] and, in particular, its new Sect. 2.6.1). As a starting point, an interesting line of research would then be to connect the application-aware paradigm with both vCCA and vCCA^D security notions by defining new weaker variants of these notions, e.g. $\mathcal{F}_C$-vCCA and $\mathcal{F}_C$-vCCA^D security, for leveraging somewhat correct (and CPA) or CPA^D schemes, i.e. schemes achieving correctness or CPA^D security only over $\mathcal{F}_C$, to CCA security levels. For example, the vCCA$_{\text{SC}}$ and vCCA^D decryption oracles may further check that $f \notin \mathcal{F}_C$ in conditions (7) and (8), respectively (which is precisely what is suggested for the CPA^D game evaluation oracle in [1]). Our intuitions are that the picture depicted in this paper will be relatively similar for these restricted security notions but we leave this for further work. However, a difficult point will be to capture the dependency of the application aware approach upon noise estimation strategies in meaningful CCA security notions, with the hope of achieving both beyond CCA1 security and relieving the library users of the burden of enforcing by hand the constraints of that paradigm.

References

1. Alexandru, A., Badawi, A.A., Micciancio, D., Polyakov, Y.: Application-aware approximate homomorphic encryption: Configuring FHE for practical use. Tech. Rep. 203, IACR ePrint (2024)
2. Badawi, A.A., Bates, J., Bergamaschi, F., Cousins, D.B., Erabelli, S., Genise, N., Halevi, S., Hunt, H., Kim, A., Lee, Y., Liu, Z., Micciancio, D., Quah, I., Polyakov, Y., Saraswathy, R.V., Rohloff, K., Saylor, J., Suponitsky, D., Triplett, M., Vaikuntanathan, V., Zucca, V.: Openfhe: Open-source fully homomorphic encryption library. In: WAHC. pp. 53–63 (2022)
3. Bellare, M., Desai, A., Jokipii, E., Rogaway, P.: A concrete security treatment of symmetric encryption. In: SFCS. pp. 394–403 (1997)
4. Bellare, M., Desai, A., Pointcheval, D., Rogaway, P.: Relations among notions of security for public-key encryption schemes. In: CRYPTO. pp. 26–45 (1998)
5. Brakerski, Z.: Fully homomorphic encryption without modulus switching from classical gapsvp. In: CRYPTO. pp. 868–886 (2012)
6. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (leveled) fully homomorphic encryption without bootstrapping. ACM TOCT pp. 1–36 (2014)
7. Checri, M., Sirdey, R., Boudguiga, A., Bultel, J.P.: On the practical CPAD security of "exact" and threshold FHE schemes. In: CRYPTO (2024)
8. Cheon, J.H., Choe, H., Passelègue, A., Stehlé, D., Suvanto, E.: Attacks against the IND-CPAD security of exact FHE schemes. Tech. Rep. 127, IACR ePrint (2024)
9. Cheon, J.H., Kim, A., Kim, M., Song, Y.: Homomorphic encryption for arithmetic of approximate numbers. In: ASIACRYPT, pp. 409–437 (2017)

10. Chillotti, I., Gama, N., Georgieva, M., Izabachène, M.: Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In: ASIACRYPT (2016)
11. Dwork, C., Naor, M., Reingold, O.: Immunizing encryption schemes from decryption errors. In: EUROCRYPT. pp. 342–360 (2004)
12. Fan, J., Vercauteren, F.: Somewhat practical fully homomorphic encryption. IACR ePrint (2012)
13. Ganesh, C., Nitulescu, A., Soria-Vazquez, E.: Rinocchio: Snarks for ring arithmetic. J. Cryptol. p. 41 (2023)
14. Grivet-Sébert, A., Checri, M., Stan, O., Sirdey, R., Gouy-Pailler, C.: Combining homomorphic encryption and differential privacy in federated learning. In: IEEE PST. pp. 1–7 (2023)
15. Grivet-Sébert, A., Pinot, R., Zuber, M., Gouy-Pailler, C., Sirdey, R.: SPEED: secure, private, and efficient deep learning. Machine Learning pp. 675–694 (2021)
16. Grivet-Sébert, A., Zuber, M., Stan, O., Sirdey, R., Gouy-Pailler, C.: A probabilistic design for practical homomorphic majority voting with intrinsic differential privacy. In: WAHC. pp. 47–58 (2023)
17. Guo, Q., Nabokov, D., Suvanto, E., Johansson, T.: Key recovery attacks on approximate homomorphic encryption with nonworst-case noise flooding countermeasures. In: Usenix Security (2024)
18. Li, B., Micciancio, D.: On the security of homomorphic encryption on approximate numbers. In: EUROCRYPT. pp. 648–677 (2021)
19. Li, B., Micciancio, D., Schultz, M., Sorrell, J.: Securing approximate homomorphic encryption using differential privacy. In: CRYPTO. pp. 560–589 (2022)
20. Manulis, M., Nguyen, J.: Fully homomorphic encryption beyond IND-CCA1 security: Integrity through verifiability. In: EUROCRYPT. pp. 63–93 (2024)
21. Naor, M., Yung, M.: Public-key cryptosystems provably secure against chosen ciphertext attacks. In: ACM STOC. pp. 427–437 (1990)

A Formal preliminaries on SNARKs

Let us recall the formal definition of (zero-knowledge) succinct non-interactive arguments of knowledge (zk-SNARKs), for a Boolean relation $\mathcal{R}$ on words or statements u and witnesses w, of an $\mathcal{NP}$ language. The $\mathcal{NP}$ language L being defined as $L = \{u | \exists w, \mathcal{R}(u, w) = \mathsf{True}\}$.

Definition 26 (SNARK). *A SNARK Π is defined by three algorithms,*

Setup$(1^\lambda, \mathcal{R})$**:** *on input 1^λ and an $\mathcal{NP}$ relation $\mathcal{R}$, the generation algorithm outputs a common reference string* crs*, assumed to be used in both subsequent algorithms. It can optionally output a verification key* vk *that is secret in the case of designater-verifier SNARK;*

Prove(u, w)**:** *given an instance u and a witness w such that $\mathcal{R}(u, w) =$ True, this algorithm produces a proof π;*

Verify$([\mathsf{vk}], u, \pi)$**:** *on, the optional verification key* vk*, an instance u, and a proof π, the verifier algorithm outputs* False *(reject) or* True *(accept);*

satisfying the following properties:

Correctness. *For any $u \in L$, with witness w,*

$$\Pr\left[\mathcal{V}([\mathsf{vk}], u, \pi) = \mathsf{False} \,\middle|\, \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, \mathcal{R}), \pi \leftarrow \mathsf{Prove}(u, w)\right] = neg(\lambda);$$

Succintness. *The size of the proof is linear in the security parameter λ, i.e. independent of the size of the computation or the witness;*

Knowledge-Soundness. *For any PPT adversary $\mathcal{A}^{\mathsf{ks}}$ there exists a PPT extractor $\mathcal{E}_{\mathcal{A}}$ such that:*

$$\Pr\left[\begin{array}{c} \mathsf{Verify}([\mathsf{vk}], u, \pi) = \mathsf{True} \\ \wedge\ \mathcal{R}(u, w) = \mathsf{False} \end{array} \middle| \begin{array}{r} \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, \mathcal{R}) \\ ((u, \pi), \mathsf{aux}) \leftarrow \mathcal{A}^{\mathsf{ks}}(\mathsf{crs}) \\ w \leftarrow \mathcal{E}_{\mathcal{A}}(\mathsf{crs}, (u, \pi), \mathsf{aux}) \end{array}\right] = neg(\lambda).$$

Intuitively, this means that for any prover able to produce a valid proof π for a statement u in the language, there exists an efficient extractor that outputs a witness w for the given statement u, from a trace aux of the execution of the adversary;

In case of Designated-Verifier SNARK, the adversary is given access to a verification oracle.

Zero Knowledge. *There exists a stateful interactive polynomial-size simulator $\mathsf{Sim} = (\mathsf{Simcrs}, \mathsf{SimProve})$ such that for all stateful interactive distinguishers $\mathcal{D}$, the two probabilities are negligibly close:*

$$\begin{aligned} &\Pr[\mathcal{R}(u, w) = \mathsf{True} \wedge \mathcal{D}(\pi) = 1 \,|\, \mathsf{crs} \leftarrow \mathsf{Setup}(1^\lambda, \mathcal{R}), (u, w) \leftarrow \mathcal{D}(\mathsf{crs}), \\ &\qquad\qquad \pi \leftarrow \mathsf{Prove}(u, w)]; \\ &\Pr[\mathcal{R}(u, w) = \mathsf{True} \wedge \mathcal{D}(\pi) = 1 \,|\, (\mathsf{crs}, \mathsf{trap}) \leftarrow \mathsf{Simcrs}(1^\lambda), (u, w) \leftarrow \mathcal{D}(\mathsf{crs}), \\ &\qquad\qquad \pi \leftarrow \mathsf{SimProve}(\mathsf{crs}, \mathsf{trap}, u)]. \end{aligned}$$

We stress that the above notation of extractor $\mathcal{E}_{\mathcal{A}}$ limits to a **straightline extractability** (without possible rewinding), but this is what we will need.