

A Unified Treatment of Anamorphic Encryption

Wonseok Choi^{1,2}, Daniel Collins^{3*}, Xiangyu Liu^{1,2}, and Vassilis Zikas¹

¹ Georgia Institute of Technology

² Purdue University

³ Texas A&M University

wonseok@purdue.edu, danielpatcollins@gmail.com,
liu3894@purdue.edu, vzikas@gatech.edu

Abstract. Receiver anamorphic encryption (hereafter anamorphic encryption), introduced by Persiano et al. at Eurocrypt 2022, allows for a double message to be symmetrically hidden in a public-key encryption ciphertext via a pre-shared *double key*. In anamorphic encryption, confidentiality must be preserved even if the adversary (or the *dictator*) has access to all regular keys. It has been the subject of several works since its introduction that explore tweaks and extensions to the core primitive. However, this study has not been systematic, and so disparate security notions have been proposed, for which their relationships are not clear. Moreover, there are clear gaps in the literature, including in the treatment of chosen-ciphertext attacks.

In this work, we conduct a systematic study of receiver anamorphic encryption. We unify existing security notions and propose several new ones, and prove implications and separations between them. Our main findings are as follows. First, we identify gaps in previous security notions against an anamorphic *sender*, namely an adversary who is given the double key, and propose three new security notions to bridge these gaps. We also identify several gaps in the treatment of chosen-ciphertext attacks, a setting only very recently considered in anamorphic cryptography (Jaeger and Stracovsky, Asiacrypt 2024). Moreover, observing that no previous construction achieves all desirable security properties in this setting, we propose a suitable construction that does. Finally, we propose several security notions for *asymmetric* anamorphic encryption, and explore the case here where the dictator and the anamorphic sender collide.

1 Introduction

Encryption has been under threat from governments around the globe for decades, from export restrictions that are tantamount to rendering the cryptography useless, the Clipper chip of the 1990s [13], to proposals made as recently as this year to ban or restrict the usage of end-to-end encryption [30].

* Work partially completed while Daniel was at Georgia Institute of Technology and Purdue University.

Supposing that end-to-end encryption is indeed outlawed or heavily monitored in a given jurisdiction, a natural question is to study to what extent secure communication can still take place. To deal with this problem, (receiver) anamorphic encryption (AME) was proposed by Persiano et al. [24] as a way for parties to secretly communicate even in the presence of a dictator who can compromise the secrets of users.⁴

An AME scheme is a standard (public-key) encryption scheme $\Pi = (\text{KGen}, \text{Enc}, \text{Dec})$ associated with an anamorphic triplet $\Sigma = (\text{aKGen}, \text{aEnc}, \text{aDec})$. If the anamorphic mode is deployed, then anamorphic key generation outputs a double key dk in addition to the usual public-secret key pair (pk, sk) . Given parties can exchange dk out-of-band, dk can then be used to carry an anamorphic message (or double message) $\hat{\text{m}}$ alongside the normal message m via anamorphic encryption $\text{aEnc}(\text{pk}, \text{dk}, \text{m}, \hat{\text{m}})$. An anamorphic ciphertext can then be both normally decrypted to m using sk , or be decrypted to $\hat{\text{m}}$ using dk (and sometimes, including this work, also with sk , i.e., $\text{aDec}(\text{sk}, \text{dk}, \text{ct})$).

Since the initial work of Persiano et al. was published, there has been a flurry of research on anamorphic encryption. These works consider important extensions and instantiations of anamorphic encryption. Some works examine what kind of security can be provided against a dictator, including *robustness* [1], ensuring that regular encryptions must fail to be anamorphically decrypted, and more generally chosen ciphertext attacks [17]. Some consider security against an anamorphic *sender* who compromises the double key but not the PKE secret key. Related to this, *asymmetric* anamorphic encryption (AAME) has been proposed, where the sender and receiver each have a different double key. Other aspects, which we do not explore further in this work, include sender anamorphic encryption [24,29], homomorphic anamorphic encryption [8], and anamorphic signatures [19].

In general, existing work focuses itself on specific aspects or extensions of anamorphic encryption. However, it is paramount to understand the relationship between different notions of security, and what meaningful security notions may exist. Moreover, by exploring the landscape of possible from a higher level, we are able to understand exactly what security *should* be provided for anamorphic encryption, i.e., the strongest possible. For example, chosen ciphertext attacks, the gold standard for ‘regular’ encryption, were only considered in one very recent work on anamorphic cryptography, and not in a systematic fashion. This methodology has proven highly successful in previous studies of fundamental primitives like public key encryption, authenticated encryption, and garbled circuits [3,5,4]. We therefore take a step back and ask the following question:

What are the ‘right’ security notions for anamorphic encryption?

⁴ They further consider so-called *sender anamorphic encryption* which is beyond the scope of this work.

1.1 Contributions and Technical Overview

In this work, we provide a systematic treatment of receiver-anamorphic encryption. We systematize existing definitions, and, thanks to this perspective, provide new ones where we deem appropriate. We summarise the definitions that we consider in Table 1, many of which have been considered before but notably some that have not. We further prove both relations and non-implications between these notions; we summarise our findings in Fig. 1. We analyse which of these security notions are satisfied by existing constructions in Table 2. Notably, some of our notions are not satisfied by *any* existing approach to build anamorphic encryption that we are aware of; we therefore propose constructions, both for anamorphic encryption and asymmetric anamorphic encryption, to bridge this gap.

Security Notions	Attacking Goal	$\mathcal{A}$'s Info.	$\mathcal{A}$'s Oracles
IND-CPA	$\text{Enc}(m_0) \approx \text{Enc}(m_1)$	$\text{pk} // \text{KGen}(1^\lambda)$	$\perp$
sk-dualCPA [24]	Normal Mode $\approx$ Anam. Mode $\text{Enc}(m) \approx \text{aEnc}(m, \hat{m})$	$\text{pk}, \text{sk} // \begin{matrix} \text{KGen}(1^\lambda) \text{ in NM} \\ \text{aKGen}(1^\lambda) \text{ in AM} \end{matrix}$	$\perp$
sk-aCPAa [24]	$\text{aEnc}(m, \hat{m}_0) \approx \text{aEnc}(m, \hat{m}_1)$	$\text{pk}, \text{sk} // \text{aKGen}(1^\lambda)$	$\text{AEnc}(\text{pk}, \text{dk}, \cdot, \cdot)$
dk-CPA-AM (new)	$\text{Enc}(m_0) \approx \text{Enc}(m_1)$	$\text{pk}, \text{dk} // \text{aKGen}(1^\lambda)$	$\perp$
dk-aCPAn (Single-AnG [20])	$\text{aEnc}(m_0, \hat{m}) \approx \text{aEnc}(m_1, \hat{m})$	$\text{pk}, \text{dk} // \text{aKGen}(1^\lambda)$	$\perp$
dk-aCPAa (new)	$\text{aEnc}(m, \hat{m}_0) \approx \text{aEnc}(m, \hat{m}_1)$	$\text{pk}, \text{dk} // \text{aKGen}(1^\lambda)$	$\perp$
dk-aCPA+ (new)	$\text{aEnc}(m_0, \hat{m}_0) \approx \text{aEnc}(m_1, \hat{m}_1)$	$\text{pk}, \text{dk} // \text{aKGen}(1^\lambda)$	$\perp$
ROB-PT (Robustness [1])	$\text{aDec}(\text{sk}, \text{dk}, \text{Enc}(m)) \approx \perp$	$\text{pk}, \text{sk} // \text{aKGen}(1^\lambda)$	$\perp$
ROB-CT (new)	$\text{aDec}(\text{sk}, \text{dk}, \text{ct}) \approx \perp // \text{ct from } \mathcal{A}$	$\text{pk}, \text{sk} // \text{aKGen}(1^\lambda)$	$\perp$
ROB-CT+ ([17]/new)	$\text{aDec}(\text{sk}, \text{dk}, \text{ct}) \approx \perp // \text{ct from } \mathcal{A}$	$\text{pk}, \text{sk} // \text{aKGen}(1^\lambda)$	$\text{AEnc}(\text{pk}, \text{dk}, \cdot, \cdot)$
IND-CCA	$\text{Enc}(\text{pk}, m_0) \approx \text{Enc}(\text{pk}, m_1)$	$\text{pk} // \text{KGen}(1^\lambda)$	$\text{Dec}(\text{sk}, \cdot)$
sk-dualCCA (new)	Normal Mode $\approx$ Anam. Mode $\text{Enc}(m) \approx \text{aEnc}(m, \hat{m})$	$\text{pk}, \text{sk} // \begin{matrix} \text{KGen}(1^\lambda) \text{ in NM} \\ \text{aKGen}(1^\lambda) \text{ in AM} \end{matrix}$	$\perp$ in NM $\text{ADec}(\text{sk}, \text{dk}, \cdot)$ in AM
sk-aCCAa ([17]/new)	$\text{aEnc}(m, \hat{m}_0) \approx \text{aEnc}(m, \hat{m}_1)$	$\text{pk}, \text{sk} // \text{aKGen}(1^\lambda)$	$\text{AEnc}(\text{pk}, \text{dk}, \cdot, \cdot)$ $\text{ADec}(\text{sk}, \text{dk}, \cdot)$
dk-CCA-AM (new)	$\text{Enc}(m_0) \approx \text{Enc}(m_1)$	$\text{pk}, \text{dk} // \text{aKGen}(1^\lambda)$	$\text{Dec}(\text{sk}, \cdot)$ $\text{ADec}(\text{sk}, \text{dk}, \cdot)$
dk-aCCAn (new)	$\text{aEnc}(m_0, \hat{m}) \approx \text{aEnc}(m_1, \hat{m})$	$\text{pk}, \text{dk} // \text{aKGen}(1^\lambda)$	$\text{Dec}(\text{sk}, \cdot)$ $\text{ADec}(\text{sk}, \text{dk}, \cdot)$
dk-aCCAa (new)	$\text{aEnc}(m, \hat{m}_0) \approx \text{aEnc}(m, \hat{m}_1)$	$\text{pk}, \text{dk} // \text{aKGen}(1^\lambda)$	$\text{Dec}(\text{sk}, \cdot)$ $\text{ADec}(\text{sk}, \text{dk}, \cdot)$
dk-aCCA+ (new)	$\text{aEnc}(m_0, \hat{m}_0) \approx \text{aEnc}(m_1, \hat{m}_1)$	$\text{pk}, \text{dk} // \text{aKGen}(1^\lambda)$	$\text{Dec}(\text{sk}, \cdot)$ $\text{ADec}(\text{sk}, \text{dk}, \cdot)$

Table 1. Table of CPA, robustness and CCA security notions for symmetric AME scheme $\text{AME} = (\Pi, \Sigma)$ with $\Pi = (\text{KGen}, \text{Enc}, \text{Dec})$ and $\Sigma = (\text{aKGen}, \text{aEnc}, \text{aDec})$. For simplicity we omit the input pk in aEnc and pk, dk in aEnc in the second column. Notions in blue are strongest and therefore most desirable.

Security Against the Anamorphic Sender. We identify several gaps in security definitions for anamorphic encryption schemes. In particular, we observe

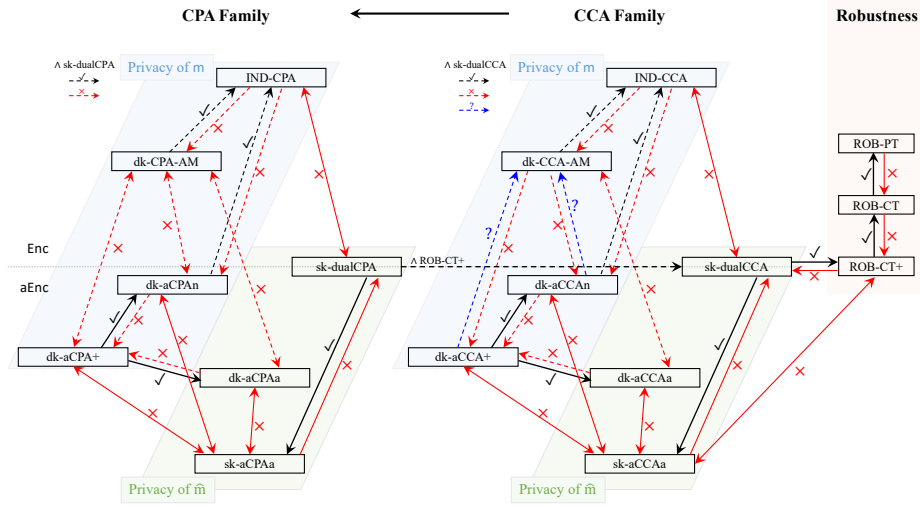


Fig. 1. Relationships among different security notions for symmetric AME. “ $A \xrightarrow{\checkmark} B$ ” indicates that A implies B , while “ $A \xrightarrow{\times} B$ ” indicates that the implication is impossible. “ $A \xrightarrow{?} B$ ”, “ $A \xrightarrow{-\checkmark} B$ ”, and “ $A \xrightarrow{-\times} B$ ” indicate that conditioned on C (which, in CPA family denotes sk-dualCPA , and in CCA family denotes sk-dualCCA), A implies B , A does not imply B , or the relationship is unknown, respectively.

that security against an anamorphic sender (where the double key is leaked) has been less explored than against a dictator (where the secret key is leaked). To bridge this gap, we define three new security notions in the CPA setting as follows (cf. Table 1).

- dk-CPA-AM security: Given the public key pk and the double key dk (i.e., the scheme is in anamorphic mode), a normal message m in a normal ciphertext generated via $\text{Enc}(\text{pk}, m)$ remains confidential under chosen-plaintext attacks.
- dk-aCPAa security: Given the public key pk and the double key dk , the anamorphic message $\hat{m}$ in an anamorphic ciphertext generated via $\text{aEnc}(\text{pk}, \text{dk}, m, \hat{m})$ remains confidential.
- dk-aCPA+ security: Given the public key pk and the double key dk , the normal message m and the anamorphic message $\hat{m}$ in an anamorphic ciphertext generated via $\text{aEnc}(\text{pk}, \text{dk}, m, \hat{m})$ remain confidential.

We argue that these new notions do not imply nor are implied by existing security notions, including standard IND-CPA security, sk-dualCPA security (the core Receiver-AM notion in [24], where the normal mode and anamorphic mode are indistinguishable to the dictator), and dk-aCPAn security [20] (the normal message in an anamorphic ciphertext is hidden to the anamorphic sender).

As shown in Fig. 1, we conduct a systematic study on the relationships among security notions of AME, highlighting that the security against the dictator

Approaches \ Security	sk-dualCPA	dk-CPA-AM	dk-aCPA+	ROB-PT	ROB-CT+	sk-dualCCA	dk-CCA-AM	dk-aCCA+
Symmetric AME								
Rejection Sampling ^a [24,9]	✓	✓	×	×	×	×	×	×
rr-PKE [20,17]	✓	✓	✓	✓	✓*	×	△	△
ElGamal [20]	✓	×	×	△	×	×	×	×
SPH [20]	✓	×	×	✓	×	×	×	×
PRF-based Scheme [1,17]	✓	✓	×	✓	✓*	×	×	×
Hybrid Encryption [8]	✓	✓	✓	✓	×	×	△	△
IBE-PKE [8]	✓	✓	✓	✓	×	×	✓	✓
Our Scheme (Sec. 5.4)	✓	✓	✓	✓	✓	✓	✓	✓
Asymmetric AME								
NY Paradigm [24]	✓	✓	✓	✓	△	△	×	×
CS PKE [20,1]	✓	✓	✓	✓	×	×	×	×
KW PKE [10]	✓	✓	✓	✓	×	×	✓	✓
Our Scheme (Sec. 6.2)	✓	✓	✓	✓	✓	✓	✓	✓

Table 2. Analysis of existing approaches to build AME. rr-PKE denotes randomness-recovering PKE. Some of what is listed in the table are generic compilers/paradigms, where security relies on the security of the underlying building blocks. “△” denotes that the scheme can be enhanced to achieve the specified security notion, but it was not addressed in the original paper. “✓*” refers to the enhanced transforms proposed in the full version of [17], which, like us, additionally propose sk-aCCAA-secure schemes.

^a A limitation of black-box rejection sampling has recently been identified in [9].

(notions of the form sk-X) and security against the anamorphic sender (notions of form dk-X) are incomparable, due to the different roles that the secret key **sk** and the double key **dk** play.

Security of AME in the CCA Setting. We extend all security notions to consider chosen-ciphertext attacks (CCA). In particular, we formalise sk-dualCCA security in the CCA setting, a strictly stronger but more reasonable notion than the widely-applied sk-dualCPA notion [24]:

- sk-dualCCA security: Given the secret key **sk**, the adversary (the dictator) cannot distinguish whether the cryptosystem is operating in normal or anamorphic mode, even in the presence of a CCA oracle.

We highlight that no existing AME scheme we are aware of achieves sk-dualCCA security (see Table 2). Moreover, we extend all CPA security notions that we consider to the CCA setting, including sk-aCCAA, dk-CCA-AM and dk-aCCA(n/a/+) security (respectively). We systematically investigate the relationships among these security notions, including their connection with robustness [1]. To address the insufficiency of the existing notion of robustness, we consider two stronger variants, namely ROB-CT security and ROB-CT+ security, building upon the robustness notion defined in [1]. We further explore their relationships with CPA and CCA security of AME (see Fig. 1), and in particular show that a scheme that is sk-dualCPA and ROB-CT+ secure is also sk-dualCCA secure, analogous to the well-known result that privacy and ciphertext integrity implies IND-CCA security for authenticated encryption [5].

Relationships Between Security Notions. As summarised in Fig. 1, in this work we show relationships between many security notions, and prove that some (sometimes in combination) do not imply others. This is not always straightforward. For example, observe first that dk-aCPA+ and dk-CPA-AM do not imply each other, since the first is concerned with indistinguishability of aEnc and the second with Enc . By careful construction of counterexamples, we show that this is still the case *even when* sk-dualCPA additionally holds, i.e. dk-aCPA+ (resp. dk-CPA-AM) $\wedge$ $\text{sk-dualCPA} \not\Rightarrow \text{dk-CPA-AM}$ (resp. dk-aCPA+). Interestingly, we show that if (pk, sk) and dk are independent, then $\text{dk-aCPA+} \wedge \text{sk-dualCPA} \Rightarrow \text{dk-CPA-AM}$ holds, but this *still* doesn't hold when replacing the roles of dk-aCPA+ and dk-CPA-AM , highlighting the subtleties inherent to comparing security notions. We refer the reader to Section 4.2 for all of the details.

Constructions Achieving All Security Properties. We propose a generic paradigm for designing secure AME schemes which satisfies the strongest variants of our security notions — sk-dualCCA , dk-CCA-AM and dk-aCCA+ — simultaneously, namely from a randomness-recovering PKE (rr-PKE) scheme. Though rr-PKE schemes have been shown to admit anamorphic triplets in [20], the generic compiler of [20] is not secure in the CCA setting. We enhance the compiler to achieve these three security notions simultaneously, leveraging the encode-then-encipher paradigm [6] in the ideal cipher model. We believe that sk-dualCCA , dk-CCA-AM and dk-aCCA+ should be targeted whenever possible. We leave exploring additional approaches to satisfying these notions as important future work.

Collusion Issues in the Asymmetric Setting. In the asymmetric AME setting where the double key is divided into the sender double key sdk (held by the anamorphic sender for anamorphic encryption) and the receiver double key rdk (held by the anamorphic receiver for anamorphic decryption), we further consider security against a powerful adversary who compromises both the secret key sk and the sender double key sdk . We formalize four security notions in this context: sk-sdk-dualCPA and sk-sdk-aCPAa in the CPA setting, and sk-sdk-dualCCA and sk-sdk-aCCAa in the CCA setting. We then adapt the generic compiler from rr-PKE schemes to this asymmetric setting to achieve sk-sdk-dualCCA security (and hence sk-sdk-aCCAa security).

Comparison with [17]. In concurrent work, Jaeger and Stracovsky propose new security notions for anamorphic signatures (and encryption in the full version). Our work is primarily focused on enumerating and exploring relations between security notions, proposing constructions as feasibility results or counterexamples along the way. By comparison, [17] mainly consider which of the definitions that they propose are satisfied by schemes from the literature on anamorphic cryptography (we do so in Table 2), and conduct only a preliminary investigation of relations between security notions. In the full version of their work, they map their results to the encryption setting, culminating in their proof of the relation $\text{sk-aCPA} \wedge \text{ROB-CT+} \Rightarrow \text{sk-aCCAa}$ (whereas in this work

we show $\text{sk-dualCPA} \wedge \text{ROB-CT+} \Rightarrow \text{sk-dualCCA}$). See Appendix E for additional comparison between our work and theirs.

1.2 Roadmap

This paper is organized as follows. Below, in Section 2, we first motivate our treatment of different adversarial settings further and provide an additional overview of our work. We introduce basic notation in Section 3. In Section 4 we examine security notions for symmetric AME, namely the strongest notions, dk-dualCPA, dk-CPA-AM and dk-aCPA+ security. In Section 5, we consider ROB-PT and ROB-CT+ security, extend the security notions from the CPA setting to the CCA setting, and illustrate how a randomness recovering PKE (rr-PKE) scheme can be extended to an AME scheme satisfying all of the strongest security properties we define. In Section 6 we consider the security of asymmetric AME, focusing on security against the collusion of the dictator and the anamorphic sender, and extend our construction from the previous section to this setting.

In the Supplementary Material, we first provide additional background on public-key encryption, symmetric encryption, and provide related preliminaries (Appendix A). Due to space limitations, we provide the remainder of our treatment of AME, including formal definitions and relationships between different notions, in Appendices B, C and D. Finally, further discussion and insights are provided in Appendix E.

2 Motivation and Overview

The initial work of [24] spawned a fruitful line of work on AME that shows that many well-known encryption schemes admit anamorphic triplets (like the Naor-Yung paradigm [24], the Cramer-Shoup CCA encryption scheme [20], and the hybrid encryption paradigm [8], to name a few). While most previous works focused on providing security against the dictator, only a few works [20,8,17] considered the security against an anamorphic sender or senders. Recall that AME involves four distinct parties: the receiver (who runs key generation), the dictator, the anamorphic sender(s), and the eavesdroppers. Security against eavesdroppers is addressed by standard IND-CPA (or IND-CCA) security, while security against the dictator was first formalized in [24] and has been followed up in subsequent work [1,8,20,25].

Anamorphic Sender: Trusted Ally, or Potential Attacker? An encryption scheme (either a normal encryption scheme or an anamorphic triplet; see above for our definitions) is deployed by the receiver who samples the public key, secret key, and possibly a double key, and wishes to ensure that messages sent to them are confidential. Suppose under coercion that the receiver hands over their secret key sk to the dictator so that the dictator can read all messages concealed in ciphertexts sent to the receiver. In anamorphic encryption, the receiver shares a double key privately to some anamorphic sender such that they can send double

messages to them via anamorphic encryption. However, should the receiver allow anamorphic senders to read *normal* messages inside of ciphertexts? We argue that they should *not* unless they also have access to the secret key.

Consider a concrete example, the ElGamal anamorphic triplet of Kutyłowski et al. [20], where the double key consists of a symmetric key K and the secret key x of public key $X = g^x$. In other words, the anamorphic sender holding the double key $\mathbf{dk}$ is able to read all (normal) messages and potential anamorphic messages in ciphertexts initially sent to the receiver. In other words, sharing the double key poses a significant threat to the security of the receiver – if several senders hold the anamorphic key, then each sender can read all regular messages! Moreover, mitigating this by forcing the receiver to share a different anamorphic key with each party not only scales poorly, but also is less likely to even be possible in some scenarios. This raises the following question:

Q1: Does the double key alone compromise the confidentiality of the normal and/or anamorphic message, in either a normal or anamorphic ciphertext, and, if so, to what extent can we avoid this?

To the best of our knowledge, only two works [20,8] considered security against the anamorphic sender.⁵ Kutyłowski et al. [20] examined the security of anamorphic messages against the anamorphic sender, and Catalano, Giunta, and Migliaro [8] considered so-called “fully asymmetric security” (and only for *asymmetric* AME) where an anamorphic encryption of $(\mathbf{m}_0, \hat{\mathbf{m}}_0)$ is indistinguishable from an anamorphic encryption of $(\mathbf{m}_1, \hat{\mathbf{m}}_1)$ to the anamorphic sender.

However, there are still some natural security properties that have not been considered. For example, what security can we claim under double key (but not secret key) compromise about normal ciphertexts produced via normal encryption, or the confidentiality of anamorphic messages inside anamorphic ciphertexts?

In this work, we fill this gap by proposing three new security notions against an anamorphic sender, namely $\mathbf{dk}$ -CPA-AM (protecting messages in regular encryptions in the anamorphic mode), $\mathbf{dk}$ -aCPAa (protecting anamorphic messages), and $\mathbf{dk}$ -aCPA+ (protecting regular *and* anamorphic messages in anamorphic encryptions) security, as described above. Our notions are interesting as they highlight that anamorphic encryption, where parties hold a *symmetric* double key, can provide *public key* security guarantees (i.e., a holder of $\mathbf{dk}$ alone can send but not receive). As we will see, we can attain even stronger security when the double key is *asymmetric*.

AME under Chosen-Ciphertext Attacks. In (public-key) encryption, the gold standard for security is IND-CCA2 security, i.e., security even if the adversary has access to a decryption oracle that takes as input some (potentially adversarial) ciphertext and returns its decryption. When considering security against the dictator, at first glance, CCA security may seem equivalent to CPA security, since the secret key $\mathbf{sk}$ is known to the dictator who can thus perform

⁵ The recent work [17] also considered the threat from the anamorphic sender, but in the signature setting.

decryption themselves. Of course in AME (under our syntax), there is anamorphic decryption that requires not only the secret key but also the double key, the latter being unknown to the dictator. Therefore, a natural question is:

Q2: To what extent can we provide security guarantees when an attacker has access to a regular and/or anamorphic decryption oracle?

Indeed if the encryption scheme is deployed via normal key generation, then there is no double key and hence no anamorphic decryption at all. Therefore, our new sk-dualCCA security notion requires that the adversary, holding the secret key sk , cannot distinguish the anamorphic mode where there is an anamorphic decryption oracle that inputs ct and returns $aDec(sk, dk, ct)$, from the normal mode where there is also a decryption oracle but always returns $\perp$.⁶

Let us see why CCA security, for example sk-dualCCA security, is practically important in more detail. Suppose that the anamorphic sender Alice sends a ciphertext ct to the receiver Bob, where ct is an anamorphic encryption of

normal message $m = \text{“Glory to the dictator!”}$,

and

anamorphic message $\hat{m} = \text{“Down with the dictator! Protest at 10 am.”}$

We assume a dictator that surveils all users by decrypting every ciphertext that is sent. Suppose that message m looks innocent and the dictator decides to pass ciphertext ct to Bob. However, due to either benign faults or modification from a suspicious dictator, ciphertext ct has been changed to another ciphertext ct' where the normal message remains the same, but the anamorphic message changes to

modified $\hat{m}' = \text{“Down with the dictator! Protest at 8 am.”}$

Then, after receiving ct' , Bob performs anamorphic decryption to obtain the modified anamorphic message $\hat{m}'$ (this modification can be unknown to the dictator), and views it as call to action from Alice. Due to the inconsistent anamorphic messages contained in ct and ct' , the use of such an anamorphic channel could be exposed to the dictator, and consequently the revolution might fail.

Relations with Robustness. To prevent a normal ciphertext from being misunderstood as containing an anamorphic message, [1] defined robustness for AME. Informally, an AME scheme has robustness if applying anamorphic decryption to a ciphertext generated from $Enc(pk, m)$ will output a failure indicator except with negligible probability. The definition of robustness has been considered in subsequent work [8,10,28] and has been regarded as a standard notion for AME schemes. It seems that sk-dualCCA security defined above is highly related to robustness, since to invalidate the anamorphic decryption oracle obtained by the adversary (the dictator), the anamorphic decryption should reject all ciphertexts produced by the adversary.

⁶ In order to achieve sk-dualCCA security, decryption cannot use *implicit rejection*.

However, robustness as defined in [1] guarantees only the robustness of ciphertexts from normal encryption, but does not require anything on *adversarial* ciphertexts. In fact, to ensure sk-dualCCA security, we need a stronger version of robustness where it is infeasible to generate a different ciphertext that could be anamorphically decrypted to a non-failure message, even given multiple anamorphic ciphertexts produced via $\text{aEnc}(\text{pk}, \text{dk}, \text{m}, \hat{\text{m}})$ with $\text{m}, \hat{\text{m}}$ chosen by the adversary. We call this stronger notion ROB-CT+, which is a necessary condition for sk-dualCCA security.

Despite the strength of sk-dualCCA, we emphasize that no existing AME schemes as stated achieve this property. That means the use of an anamorphic channel is in fact unsafe against a dictator making CCA attacks.

Moreover, we believe that threats against the anamorphic sender should also be considered in the CCA setting. Since in our treatment the anamorphic sender has access to the double key dk but not the secret key sk (which, as observed above, is not always true for anamorphic encryption [24,1], but is more general), the latter being required in both normal decryption and anamorphic decryption, the anamorphic sender (as the adversary) is provided with both a normal and anamorphic decryption oracle. Consequently, we extend the security notion of dk-CPA-AM and dk-CPA(n/a/+) in the CPA setting to dk-CCA-AM and dk-CCA(n/a/+) in the CCA setting, respectively.

Asymmetric AME: Security Against Collusion. In the typical formulation of anamorphic encryption, the double key is assumed to be a symmetric key shared between the anamorphic sender and the receiver [24,1]. Later works [20,8,10] considered the scenario that the double key held by the anamorphic sender, used for anamorphic encryption, in general *differs* from the double key held by the receiver used for anamorphic decryption. We call this an asymmetric AME (AAME) scheme, and denote the sender double key by sdk and the receiver double key by rdk . Symmetric AME can be viewed as a special case of AAME when $\text{dk} = \text{sdk} = \text{rdk}$.

While most security notions are similar between the symmetric case and the asymmetric case, we study the following strong security requirement:

*Q3: What if a powerful adversary gains both the secret key sk and the sender double key sdk ? What security can be provided in this scenario?*⁷

The case that the adversary obtains both sk and sdk happens if the dictator and the anamorphic sender collude. In this scenario, the powerful adversary not only knows that the encryption scheme was deployed in the anamorphic mode (due to sdk), but also has access to the normal messages in both normal ciphertexts and anamorphic ciphertexts (due to sk). However, the adversary still does not know the anamorphic message concealed in an anamorphic ciphertext, or even, does not know whether a ciphertext is anamorphic or not, since the anamorphic decryption additionally requires the receiver double key rdk which is unknown to the adversary.

⁷ Note that [8] considers sk-sdk-aCPAa security, but does not explore additional notions.

One may wonder what is the meaning of considering such a strong attack model. Consider a receiver leading an underground resistance movement against the dictator, and they deploy an (asymmetric) AME scheme so that the resistance can use `sdk` to send anamorphic messages privately to their leader. However, one member betrays the resistance and secretly hands over their `sdk` to the dictator. Before issuing an arrest warrant for the leader, the dictator aims to read anamorphic messages contained in the ciphertexts sent from other members of the movement. Furthermore, the dictator may want to identify exactly who belongs to this movement by determining whether they have sent an anamorphic ciphertext to the receiver. To prevent this, the receiver must ensure that the leakage of both `sk` and `sdk` does not compromise the confidentiality of anamorphic messages.

We consider `sk-sdk-dualCPA` and `sk-sdk-aCPAa` security (as well as `sk-sdk-dualCCA` and `sk-sdk-aCCAa` security in the CCA setting) to address this issue, and explore how to achieve those security notions. As we discuss in Section 5.4, in the randomness-recovering PKE framework, CCA-secure symmetric encryption is not sufficient for CCA-secure (symmetric) AME. Interestingly, CCA-secure PKE *is* sufficient for CCA-secure asymmetric AME, a fact we discuss in Section 6.

3 Preliminaries

We use λ to denote the security parameter which is used implicitly throughout the paper. For a distribution $\mathcal{D}$, denote by $x \leftarrow \mathcal{D}$ the operation of sampling x according to $\mathcal{D}$. For probabilistic algorithm $\mathcal{A}$, denote by $y \leftarrow \mathcal{A}(x; r)$ or $y := \mathcal{A}(x; r)$, the operation of running $\mathcal{A}$ with input x and randomness r and assigning the output to y . If the randomness is uniformly sampled, we simply denote as $y \leftarrow \mathcal{A}(x)$. For deterministic algorithms $\mathcal{A}$, we also write as $y := \mathcal{A}(x)$ or $y := \mathcal{A}(x; r)$. “PPT” is short for probabilistic polynomial-time.

We refer to Appendix A for definitions of public-key encryption (PKE), symmetric encryption (SE), authenticated encryption (AE), pseudorandom functions (PRF), ideal ciphers (IC), and their security notions.

4 Anamorphic Encryption: Syntax, Security, and More

We first consider AME in the symmetric setting, and then extend our results to the asymmetric setting in Section 6. Additional results are provided in Appendix B.

Definition 1 (Symmetric Anamorphic Encryption). *A symmetric anamorphic encryption (AME) scheme AME is a public-key encryption scheme $\Pi = (\text{KGen}, \text{Enc}, \text{Dec})$ associated with an anamorphic triplet $\Sigma = (\text{aKGen}, \text{aEnc}, \text{aDec})$. An AME has two modes: normal mode and anamorphic mode. When running the normal mode, the primitive is identical to Π . When*

running the anamorphic mode, Π is replaced by Σ where the algorithms are defined as follows:

- $(\text{pk}, \text{sk}, \text{dk}) \leftarrow \text{aKGen}(1^\lambda)$. On input the parameter λ , the anamorphic key generation algorithm outputs a public key pk , a secret key sk , and a double key dk .
- $\text{ct} \leftarrow \text{aEnc}(\text{pk}, \text{dk}, \text{m}, \hat{\text{m}})$. On input the public key pk , the double key dk , a (normal) message m and an anamorphic message $\hat{\text{m}}$, the anamorphic encryption algorithm outputs an (anamorphic) ciphertext ct .
- $\hat{\text{m}}/\perp \leftarrow \text{aDec}(\text{sk}, \text{dk}, \text{ct})$. On input the secret key sk , the double key dk , and a ciphertext ct , the anamorphic decryption algorithm outputs an anamorphic message $\hat{\text{m}}$ or a failure indicator $\perp$.

Correctness of Σ . For every (all-powerful) adversary $\mathcal{A}$, the probability

$$\Pr \left[\begin{array}{l} (\text{pk}, \text{sk}, \text{dk}) \leftarrow \text{aKGen}(1^\lambda); (\text{m}, \hat{\text{m}}) \leftarrow \mathcal{A}(\text{pk}); \\ \text{ct} \leftarrow \text{aEnc}(\text{pk}, \text{dk}, \text{m}, \hat{\text{m}}) \end{array} : \begin{array}{l} \text{aDec}(\text{sk}, \text{dk}, \text{ct}) \neq \hat{\text{m}} \\ \vee \text{Dec}(\text{sk}, \text{ct}) \neq \text{m} \end{array} \right]$$

is negligible in λ .

Remark 1 (On Correctness). Prior works [24,1,20,25] have focused solely on the correctness of anamorphic encryption (cf. the first property in Def. 1), while neglecting the correctness requirement that normal decryption applied to an honest anamorphic ciphertext should also return the regular message (cf. the second property in Def. 1). Though the correctness of normal decryption is implied by sk-dualCPA security (refer to Def. 2 below) and regular correctness of PKE, this is only true for a restricted *computational* correctness notion, namely where the messages are chosen by the adversary (rather than being universally quantified as in our notion). To clarify, our notion captures both the correctness of anamorphic decryption and the correctness of (normal) decryption. Of course, Π should also be correct (cf. Appendix A.1).

Remark 2 (On the Input of Anamorphic Decryption). By the definition in [24], the anamorphic decryption uses only the double key dk to decrypt an anamorphic ciphertext. In this work we adopt a more generalized definition by requiring aDec to use not only dk but also the secret key sk , as defined in subsequent works [20,25,8]. As shown in the following sections, this generalisation enables us to analyse the security against the anamorphic sender who holds dk but not sk in both the symmetric setting and the asymmetric setting (cf. Section 6).

Remark 3 (Anamorphic Extension v.s. Anamorphic Triplet). Banfi et al. [1] observed that it can be useful to decouple double key generation from public/secret key pair generation, e.g., to support dynamic double key generation. They call the resulting primitive an *anamorphic extension*, which is also considered in [8]. An anamorphic extension can be easily cast as an anamorphic triplet, but not vice versa.

Remark 4 (Stateful AME). Banfi et al. [1] considered a stateful variant of anamorphic encryption where aEnc and aDec may input and output a state.

This allows for different constructions and one can consider various security notions in this setting (e.g., where the state may or may not be given to the adversary, where the adversary can make oracle queries with adversarially chosen state, etc.), but we do not consider this further here.

4.1 Security Notions against the Dictator

The basic security requirement of AME is that the dictator does not know whether the encryption scheme is working in the normal mode or the anamorphic mode, which is formalized as follows.

Definition 2 (sk-dualCPA Security of AME [24]). *An AME scheme $\text{AME} = (\Pi, \Sigma)$ is sk-dualCPA-secure, if, for every PPT adversary $\mathcal{A}$, the advantage*

$$\text{Adv}_{\Pi, \Sigma}^{\text{sk-dualcpa}}(\mathcal{A}) := |\Pr[\text{sk-dualCPA}_{\Pi, \Sigma, 1}(\mathcal{A}) = 1] - \Pr[\text{sk-dualCPA}_{\Pi, \Sigma, 0}(\mathcal{A}) = 1]|$$

is negligible in λ , where the experiment $\text{sk-dualCPA}_{\Pi, \Sigma, b}(\mathcal{A})$ for $b \in \{0, 1\}$ is defined in Fig. 2.

$\text{sk-dualCPA}_{\Pi, \Sigma, b}(\mathcal{A})$:	$\text{CHAL}(\mathbf{m}, \hat{\mathbf{m}})$
1 : if $b = 0$:	1 : if chal : return $\perp$
2 : $(\text{pk}, \text{sk}) \leftarrow \text{KGen}(1^\lambda)$	2 : $\text{chal} \leftarrow \text{true}$
3 : else :	3 : if $b = 0$:
4 : $(\text{pk}, \text{sk}, \text{dk}) \leftarrow \text{aKGen}(1^\lambda)$	4 : return $\text{Enc}(\text{pk}, \mathbf{m})$
5 : $\text{chal} \leftarrow \text{false}$	5 : else :
6 : return $\mathcal{A}^{\text{CHAL}}(\text{pk}, \text{sk})$	6 : return $\text{aEnc}(\text{pk}, \text{dk}, \mathbf{m}, \hat{\mathbf{m}})$

Fig. 2. sk-dualCPA security game for AME scheme $\text{AME} = (\Pi, \Sigma)$.

Remark 5. The prior work by Persiano, Phan, and Yung [24] did not separate sk-dualCPA security as an independent property, but included it as part of the definition of a *secure* AME scheme (plus regular IND-CPA security (cf. Def. 14) and the fact that $\text{aEnc}(\text{pk}, \text{dk}, \mathbf{m}, \cdot)$ and $\text{aDec}(\text{sk}, \text{dk}, \cdot)$ form a symmetric encryption scheme for any $\mathbf{m}$). To better study the relationships among different security properties, we formalize sk-dualCPA security as above.

Remark 6 (Single Challenge v.s. Multiple Challenges). sk-dualCPA security was initially defined in the multiple-challenge setting [24], where the adversary is allowed to query CHAL up to a polynomial number of times. The adversary receives either all normal ciphertexts via Enc (if $b = 0$) or all anamorphic ciphertexts via aEnc (if $b = 1$). Via a standard hybrid argument, it is straightforward to see

that security in the single-challenge setting, as defined above, implies security in the multiple-challenge setting (with a security loss Q , the number of queries to CHAL). Since we do not focus on tightness in this work, we define sk-dualCPA in the single challenge setting to maintain consistency with the standard IND-CPA notion for PKE and the sk-aCPAa notion for AME [24].

4.2 Security Notions against the Anamorphic Sender

In this subsection we explore security properties against the anamorphic sender. We formalize the security of normal encryption against the anamorphic sender as follows.

Definition 3 (dk-CPA-AM Security of AME). *An AME scheme $\text{AME} = (\Pi, \Sigma)$ is dk-CPA-AM-secure, if, for every PPT adversary $\mathcal{A}$, the advantage*

$$\text{Adv}_{\Sigma}^{\text{dk-cpa-am}}(\mathcal{A}) := |\Pr[\text{dk-CPA-AM}_{\Sigma,1}(\mathcal{A}) = 1] - \Pr[\text{dk-CPA-AM}_{\Sigma,0}(\mathcal{A}) = 1]|$$

is negligible in λ , where the experiment $\text{dk-CPA-AM}_{\Sigma,b}(\mathcal{A})$ for $b \in \{0,1\}$ is defined in Fig. 3.

dk-CPA-AM $_{\Sigma,b}(\mathcal{A})$:	CHAL(m_0, m_1)
1 : $(pk, sk, dk) \leftarrow \text{aKGen}(1^\lambda)$	1 : if chal $\vee (m_0 \neq m_1)$: return $\perp$
2 : chal $\leftarrow$ false	2 : chal $\leftarrow$ true
3 : return $\mathcal{A}^{\text{CHAL}}(pk, dk)$	3 : return Enc(pk, m_b)

Fig. 3. dk-CPA-AM security game for AME scheme $\text{AME} = (\Pi, \Sigma)$.

We will next see that dk-CPA-AM security cannot be deduced from existing IND-CPA security and sk-dualCPA security (cf. Def. 2). Furthermore, dk-CPA-AM and dk-aCPA+ (cf. Def. 4) are incomparable.

Definition 4 (dk-aCPA+ Security of Symmetric AME). *An AME scheme $\text{AME} = (\Pi, \Sigma)$ is dk-aCPA+-secure, if, for every PPT adversary $\mathcal{A}$, the advantage*

$$\text{Adv}_{\Sigma}^{\text{dk-acpa+}}(\mathcal{A}) := |\Pr[\text{dk-aCPA+}_{\Sigma,1}(\mathcal{A}) = 1] - \Pr[\text{dk-aCPA+}_{\Sigma,0}(\mathcal{A}) = 1]|$$

is negligible in λ , where the experiment $\text{dk-aCPA+}_{\Sigma,b}(\mathcal{A})$ for $b \in \{0,1\}$ is defined in Fig. 4.

Remark 7 (Comparison with the Fully Asymmetric Security in [8]). Catalano et al. [8] defined the so-called fully asymmetric anamorphic security for *asymmetric* AME, which considered the security against the anamorphic sender in the

dk-aCPA+ $_{\Sigma,b}(\mathcal{A})$:	CHAL($m_0, m_1, \hat{m}_0, \hat{m}_1$)
1 : $(pk, sk, dk) \leftarrow \text{aKGen}(1^\lambda)$	1 : if chal $\vee (m_0 \neq m_1) \vee (\hat{m}_0 \neq \hat{m}_1)$:
2 : chal $\leftarrow$ false	2 : return $\perp$
3 : return $\mathcal{A}^{\text{CHAL}}(pk, dk)$	3 : chal $\leftarrow$ true
	4 : return $\text{aEnc}(pk, dk, m_b, \hat{m}_b)$

Fig. 4. dk-aCPA+ security game for AME scheme $\text{AME} = (\Pi, \Sigma)$.

asymmetric setting (i.e., the double key is divided into two parts, the sender double key sdk and the receiver double key rdk (which is the trapdoor in [8])). We note that the fully asymmetric anamorphic security [8] is identical to the sdk-aCPA+ security defined in Fig. 30 in the CPA setting. Additionally, the dk-aCPA+ security here can be regarded as a strictly stronger extension of the fully asymmetric anamorphic security in the symmetric setting, since dk contains both sdk and rdk and hence provides more information to the adversary.

Relations between dk-CPA-AM and dk-aCPA+. Now we want to see the relationship between dk-CPA-AM and dk-aCPA+. These two notions alone do not imply each other, since they are concerned with the indistinguishability of different encryption functions (Enc or aEnc) which may be independent. We in fact show something even stronger, namely that even conditioned on sk-dualCPA security, dk-CPA-AM does not imply dk-aCPA+ security and vice versa. This highlights how notions where the secret key sk and the double key dk are leaked are incomparable.

Theorem 1 (dk-CPA-AM $\wedge$ sk-dualCPA $\not\Rightarrow$ dk-aCPA+). *For a sk-dualCPA-secure AME scheme $\text{AME} = (\Pi, \Sigma)$, dk-CPA-AM security does not imply dk-aCPA+ security.*

Proof. Let $\widetilde{\text{PKE}}$ be an IND-CPA-secure PKE scheme, and $\widetilde{\text{SE}}$ be a PR-CT-secure symmetric encryption scheme (cf. Def. 18). We give an AME construction $\text{AME} = (\Pi, \Sigma)$ which satisfies both sk-dualCPA and dk-CPA-AM but not dk-aCPA+ as follows.

- The key generation algorithms returns $(pk, sk) \leftarrow \widetilde{\text{PKE}}.\text{KGen}(1^\lambda)$.
- The anamorphic key generation algorithm returns (pk, sk, dk) , where $(pk, sk) \leftarrow \widetilde{\text{PKE}}.\text{KGen}(1^\lambda)$, and $dk \leftarrow \widetilde{\text{SE}}.\text{KGen}(1^\lambda)$.
- The encryption algorithm returns

$$\text{ct} = (\widetilde{\text{PKE}}.\text{Enc}(pk, m) || \text{str}_1 || \text{str}_2),$$

where str_1 and str_2 are two strings randomly sampled from the ciphertext space of $\widetilde{\text{SE}}$.⁸

⁸ For simplicity, we assume the same message space and anamorphic message space, which are functions of λ , and that strings of the same length are sampled each call).

- The anamorphic encryption algorithm returns

$$\text{ct} = (\widetilde{\text{PKE}}.\text{Enc}(\text{pk}, \text{m}) || \widetilde{\text{SE}}.\text{Enc}(\text{dk}, \text{m}) || \widetilde{\text{SE}}.\text{Enc}(\text{dk}, \hat{\text{m}})).$$

Now, sk-dualCPA of AME is ensured by the ciphertext pseudorandomness (PR-CT) of $\widetilde{\text{SE}}$, and dk-CPA-AM is ensured by the IND-CPA security of $\widetilde{\text{PKE}}$ and the independence of (pk, sk) and dk . However, it is easy to see that AME does not satisfy dk-aCPA+ at all, since dk gives full access to read the normal message m in an anamorphic ciphertext. $\square$

Theorem 2 (dk-aCPA+ $\wedge$ sk-dualCPA $\nRightarrow$ dk-CPA-AM). *For a sk-dualCPA-secure AME scheme $\text{AME} = (\Pi, \Sigma)$, dk-aCPA+ security does not imply dk-CPA-AM security.*

Proof. Let $\widetilde{\text{PKE}}$ be an IND-CPA-secure PKE scheme, and $\widetilde{\text{SE}}$ be a PR-CT-secure symmetric encryption scheme (cf. Def. 18). We give an AME construction $\text{AME} = (\Pi, \Sigma)$ which satisfies both sk-dualCPA and dk-aCPA+ but not dk-CPA-AM as follows.

- The key generation algorithm returns $\text{pk} = (\text{pk}_0, \text{pk}_1)$ and $\text{sk} = \text{sk}_0$, where $(\text{pk}_b, \text{sk}_b) \leftarrow \widetilde{\text{PKE}}.\text{KGen}(1^\lambda)$ for $b \in \{0, 1\}$.
- The anamorphic key generation algorithm returns $\text{pk} = (\text{pk}_0, \text{pk}_1)$, $\text{sk} = \text{sk}_0$, and $\text{dk} = (\text{sk}_1, \text{k})$, where $(\text{pk}_b, \text{sk}_b) \leftarrow \widetilde{\text{PKE}}.\text{KGen}(1^\lambda)$ for $b \in \{0, 1\}$, and $\text{k} \leftarrow \widetilde{\text{SE}}.\text{KGen}(1^\lambda)$.
- The encryption algorithm returns

$$\text{ct} = (\text{c}_0 || \text{c}_1 || \text{c}_2) = (\widetilde{\text{PKE}}.\text{Enc}(\text{pk}_0, \text{m}) || \widetilde{\text{PKE}}.\text{Enc}(\text{pk}_1, \text{m}) || \widetilde{\text{PKE}}.\text{Enc}(\text{pk}_0, r)),$$

where r is a random string sampled from the message space of $\widetilde{\text{PKE}}$.

- The anamorphic encryption algorithm returns

$$\text{ct} = (\text{c}_0 || \text{c}_1 || \text{c}_2) = (\widetilde{\text{PKE}}.\text{Enc}(\text{pk}_0, \text{m}) || \widetilde{\text{PKE}}.\text{Enc}(\text{pk}_1, \mathbf{0}) || \widetilde{\text{PKE}}.\text{Enc}(\text{pk}_0, r)),$$

where $\mathbf{0}$ denotes an all-zero string, and $r \leftarrow \widetilde{\text{SE}}.\text{Enc}(\text{k}, \hat{\text{m}})$.

Now, sk-dualCPA of AME is ensured by the ciphertext pseudorandomness (PR-CT) of $\widetilde{\text{SE}}$ and the IND-CPA security of $\widetilde{\text{PKE}}$ under sk_0 , and dk-aCPA+ is ensured by the IND-CPA security of $\widetilde{\text{PKE}}$ under sk_0 . However, it is easy to see that AME does not satisfy dk-CPA-AM at all, since $\text{dk} = (\text{sk}_1, \text{k})$ gives full access to read the normal message m from c_1 . $\square$

Remark 8. An observation is that, if (pk, sk) and dk are independent,⁹ then we can prove dk-aCPA+ and sk-dualCPA together imply dk-CPA-AM as follows.

⁹ Note that this is not the case of anamorphic extension defined in [1], where the generation of dk may still depend on (pk, sk) .

$$\begin{aligned}
& (\text{pk}, \text{dk}, \text{Enc}(\text{pk}, m_0)) \\
& \approx (\text{pk}, \text{dk}', \text{Enc}(\text{pk}, m_0)) & // \text{ independence of } (\text{pk}, \text{sk}) \text{ and } \text{dk} \\
& \approx (\text{pk}, \text{dk}', \text{aEnc}(\text{pk}, m_0, \hat{m})) & // \text{ sk-dualCPA security} \\
& \approx (\text{pk}, \text{dk}', \text{aEnc}(\text{pk}, m_1, \hat{m})) & // \text{ dk-aCPA+ security} \\
& \approx (\text{pk}, \text{dk}', \text{Enc}(\text{pk}, m_1)) & // \text{ sk-dualCPA security} \\
& \approx (\text{pk}, \text{dk}, \text{Enc}(\text{pk}, m_1)) & // \text{ independence of } (\text{pk}, \text{sk}) \text{ and } \text{dk}
\end{aligned}$$

Here $(\text{pk}, \text{sk}, \text{dk}) \leftarrow \text{aKGen}(1^\lambda)$, and dk' is an independent double key sampled according to aKGen . Note even if (pk, sk) and dk are independent that $\text{dk-CPA-AM} + \text{sk-dualCPA} \not\Rightarrow \text{dk-aCPA+}$, due to the above example in the proof of Theorem 1.

Remark 9. Given the result holds in the CPA setting and the counterexample in the proof of Theorem 2, it seems highly likely that in the CCA setting, dk-aCCA+ and sk-dualCCA together do not imply dk-CCA-AM (see Sec. 5 for formal definitions). We were unable to construct a counterexample to show this. Intuitively, an adversary (whether holding sk or dk) might reuse (some part of) a challenge ciphertext in decryption oracles calls, which makes showing both dk-aCCA+ and sk-dualCCA hold more difficult without inadvertently also achieving dk-CCA-AM security. We leave a formal proof or refutation of our conjecture as an interesting open problem.

Theorem 3 ($\text{dk-CPA-AM} \wedge \text{sk-dualCPA} \Rightarrow \text{IND-CPA}$, and $\text{dk-CPA-AM} \not\Leftarrow \text{IND-CPA} \wedge \text{sk-dualCPA}$). *For an AME scheme $\text{AME} = (\Pi, \Sigma)$, dk-CPA-AM security and sk-dualCPA security together imply IND-CPA security. However, IND-CPA security, even combined with sk-dualCPA security, does not imply dk-CPA-AM security.*

Proof. We prove $\text{dk-CPA-AM} \wedge \text{sk-dualCPA} \Rightarrow \text{IND-CPA}$ by showing that conditioned on sk-dualCPA security, an adversary that breaks IND-CPA security can be transformed into another adversary that breaks dk-CPA-AM security.

For $b \in \{0, 1\}$, define the hybrid game $\text{Hybrid}_{\Pi, \Sigma, b}(\mathcal{A})$ which is the same as the $\text{IND-CPA}_{\Pi, b}(\mathcal{A})$ except that the public key pk is generated by $(\text{pk}, \text{sk}, \text{dk}) \leftarrow \Sigma.\text{aKGen}(1^\lambda)$ instead of $(\text{pk}, \text{sk}) \leftarrow \Pi.\text{KGen}(1^\lambda)$.

Due to sk-dualCPA security, $\text{Hybrid}_{\Pi, \Sigma, b}(\mathcal{A})$ and $\text{IND-CPA}_{\Pi, b}(\mathcal{A})$ are indistinguishable to the adversary $\mathcal{A}$ (cf. Lemma 1). Furthermore, any adversary $\mathcal{A}$ capable of distinguishing $\text{Hybrid}_{\Pi, \Sigma, 1}(\mathcal{A})$ from $\text{Hybrid}_{\Pi, \Sigma, 0}(\mathcal{A})$ (where only pk is provided to the adversary) can be directly used to distinguish $\text{dk-CPA-AM}_{\Pi, \Sigma, 1}(\mathcal{A})$ and $\text{dk-CPA-AM}_{\Pi, \Sigma, 0}(\mathcal{A})$ (where both pk and dk are provided).

The proof for the other direction $\text{dk-CPA-AM} \not\Leftarrow \text{IND-CPA} (\wedge \text{sk-dualCPA})$ is straightforward, since both IND-CPA security and sk-dualCPA security assume that the adversary are not given the double key dk . If an AME scheme

(Π, Σ) is designed such that sk is contained in dk then the normal message m is revealed immediately,¹⁰ and hence dk-CPA-AM security does not hold. $\square$

From the above theorem we can deduce that, in the CPA setting, a secure AME scheme ought to satisfy sk-dualCPA , dk-CPA-AM and dk-aCPA+ security.

5 Security of Anamorphic Encryption in the CCA Setting

In this section we explore the security of AME in the chosen-ciphertext attack (CCA) setting. Additional results in this setting are provided in Appendix C.

5.1 Robustness Notions

We first recall the definition of robustness from [1].

Definition 5 (ROB-PT Security of AME (Robustness in [1])). *An AME scheme $\text{AME} = (\Pi, \Sigma)$ is ROB-PT-secure, if, for every PPT adversary $\mathcal{A}$, the advantage*

$$\text{Adv}_{\Pi, \Sigma}^{\text{rob-pt}}(\mathcal{A}) := \Pr[\text{ROB-PT}_{\Pi, \Sigma}(\mathcal{A}) = 1]$$

is negligible in λ , where the experiment $\text{ROB-PT}_{\Pi, \Sigma}(\mathcal{A})$ is defined in Fig. 5.

ROB-PT $_{\Pi, \Sigma}(\mathcal{A})$:	
1 :	$(\text{pk}, \text{sk}, \text{dk}) \leftarrow \text{aKGen}(1^\lambda)$
2 :	$\text{m} \leftarrow \mathcal{A}(\text{pk}, \text{sk})$
3 :	if $\text{aDec}(\text{sk}, \text{dk}, \text{Enc}(\text{pk}, \text{m})) \neq \perp$: return 1
4 :	return 0

Fig. 5. ROB-PT security game for AME scheme $\text{AME} = (\Pi, \Sigma)$.

Now we consider a stronger notion ROB-CT+, where the adversary additionally has access to an anamorphic encryption oracle and can output any adversarial ciphertexts. ROB-CT+ is highly related to the CCA security of AME. We also consider an intermediate notion ROB-CT in Appendix C.

Definition 6 (ROB-CT+ Security of AME). *An AME scheme $\text{AME} = (\Pi, \Sigma)$ is ROB-CT+-secure, if, for every PPT adversary $\mathcal{A}$, the advantage*

$$\text{Adv}_{\Pi, \Sigma}^{\text{rob-ct+}}(\mathcal{A}) := \Pr[\text{ROB-CT+}_{\Pi, \Sigma}(\mathcal{A}) = 1]$$

is negligible in λ , where the experiment $\text{ROB-CT+}_{\Pi, \Sigma}(\mathcal{A})$ is defined in Fig. 6.

¹⁰ A concrete example is the ElGamal anamorphic triplet shown in [20], where the double key consists of a symmetric key K and the secret key x of the public key $X = g^x$.

ROB-CT+ $_{\Pi, \Sigma}(\mathcal{A})$:	A _{ENC} (m, $\hat{m}$)
1 : (pk, sk, dk) $\leftarrow$ aKGen(1^λ)	1 : ct $\leftarrow$ aEnc(sk, dk, m, $\hat{m}$)
2 : CT $\leftarrow \emptyset$	2 : CT $\leftarrow$ CT $\cup \{\text{ct}^*\}$
3 : ct* $\leftarrow \mathcal{A}^{\text{AENC}}(\text{pk}, \text{sk})$	3 : return ct
4 : if (aDec(sk, dk, ct*) $\neq \perp$) $\wedge$ (ct $\notin$ CT) :	
5 : return 1	
6 : return 0	

Fig. 6. ROB-CT+ security game for AME scheme $\text{AME} = (\Pi, \Sigma)$.

5.2 Security against the Dictator in the CCA Setting

Now we extend the standard sk-dualCPA security of AME (cf. Def. 2) to the CCA setting, which we call sk-dualCCA security. Informally, it states that given additionally an oracle which returns $\perp$ in the normal mode and returns the anamorphic decryption result in the anamorphic mode, the adversary (acting as the dictator) still cannot distinguish these two modes.

Definition 7 (sk-dualCCA Security of AME). *An AME scheme $\text{AME} = (\Pi, \Sigma)$ is sk-dualCCA-secure, if, for every PPT adversary $\mathcal{A}$, the advantage*

$$\text{Adv}_{\Pi, \Sigma}^{\text{sk-dualcca}}(\mathcal{A}) := |\Pr[\text{sk-dualCCA}_{\Pi, \Sigma, 1}(\mathcal{A}) = 1] - \Pr[\text{sk-dualCCA}_{\Pi, \Sigma, 0}(\mathcal{A}) = 1]|$$

is negligible in λ , where the experiment $\text{sk-dualCCA}_{\Pi, \Sigma, b}(\mathcal{A})$ for $b \in \{0, 1\}$ is defined in Fig. 7.

sk-dualCCA $_{\Pi, \Sigma, b}(\mathcal{A})$:	CHAL(m, $\hat{m}$)
1 : if $b = 0$:	1 : if ct* $\neq \perp$: return $\perp$
2 : (pk, sk) $\leftarrow$ KGen(1^λ)	2 : if $b = 0$:
3 : else :	3 : ct* $\leftarrow$ Enc(pk, m)
4 : (pk, sk, dk) $\leftarrow$ aKGen(1^λ)	4 : else :
5 : ct* $\leftarrow \perp$	5 : ct* $\leftarrow$ aEnc(pk, dk, m, $\hat{m}$)
6 : return $\mathcal{A}^{\text{CHAL}, \text{ADEC}}(\text{pk}, \text{sk})$	6 : return ct*
ADEC(ct)	
1 : if $b = 0 \vee \text{ct} = \text{ct}^*$: return $\perp$	
2 : else : return aDec(sk, dk, ct)	

Fig. 7. sk-dualCCA security game for AME scheme $\text{AME} = (\Pi, \Sigma)$.

We argue that sk-dualCCA is strictly stronger than (all) robustness notions defined in the subsection above.

Theorem 4 (sk-dualCCA $\Rightarrow$ ROB-CT+, and sk-dualCCA $\not\Leftarrow$ ROB-CT+). *For an AME scheme $\text{AME} = (\Pi, \Sigma)$, sk-dualCCA implies ROB-CT+, which in turn implies ROB-CT, and finally ROB-PT. Conversely, the implications in the opposite direction do not hold.*

Proof. The direction sk-dualCCA $\Rightarrow$ ROB-CT+ is straightforward. By Theorem 16, it is sufficient to prove that sk-dualCCA $\not\Leftarrow$ ROB-CT+.

Let $\widetilde{\text{AME}}$ be an sk-dualCCA-secure AME scheme, and therefore it is ROB-CT+-secure. Now we design a new AME scheme AME whose (anamorphic) key generation algorithm are identical to those in $\widetilde{\text{AME}}$, and

$$\begin{aligned}\text{AME.Enc}(\text{pk}, m) &:= \widetilde{\text{AME.Enc}}(\text{pk}, (0||m)), \\ \text{AME.aEnc}(\text{pk}, \text{dk}, m, \hat{m}) &:= \widetilde{\text{AME.aEnc}}(\text{pk}, \text{dk}, (1||m), \hat{m}).\end{aligned}$$

ROB-CT+ of AME is derived from ROB-CT+ of $\widetilde{\text{AME}}$. However, AME does not satisfy sk-dualCCA security (or even sk-dualCPA security), since one can easily distinguish the normal mode from the anamorphic mode with the knowledge of sk . $\square$

Now we study the relationship between sk-dualCPA and sk-dualCCA. Obviously, sk-dualCCA is strictly stronger than sk-dualCPA. On the other hand, we prove that equipped with ROB-CT+, sk-dualCPA can be enhanced to sk-dualCCA.

Theorem 5 (sk-dualCPA $\wedge$ ROB-CT+ $\Rightarrow$ sk-dualCCA). *If an AME scheme (Π, Σ) has both sk-dualCPA security and ROB-CT+ security, then it is sk-dualCCA-secure.*

Proof. It is straightforward to see that if $b = 0$, then the experiment $\text{sk-dualCCA}_{\Pi, \Sigma, 0}(\mathcal{A})$ and the experiment $\text{sk-dualCPA}_{\Pi, \Sigma, 0}(\mathcal{A})$ are identical, since the (anamorphic) decryption oracle in $\text{sk-dualCCA}_{\Pi, \Sigma, 0}(\mathcal{A})$ always returns a failure indicator, downgrading the security from CCA to CPA. Therefore, to prove sk-dualCCA security, it is sufficient to bound the distinguishing advantage between $\text{sk-dualCCA}_{\Pi, \Sigma, 1}(\mathcal{A})$ and $\text{sk-dualCPA}_{\Pi, \Sigma, 1}(\mathcal{A})$.

Suppose that the adversary $\mathcal{A}$ in $\text{sk-dualCPA}_{\Pi, \Sigma, 1}(\mathcal{A})$ is also equipped with a decryption oracle which always returns $\perp$. Therefore, $\mathcal{A}$ is able to distinguish the experiment $\text{sk-dualCPA}_{\Pi, \Sigma, 1}(\mathcal{A})$ from the experiment $\text{sk-dualCCA}_{\Pi, \Sigma, 1}(\mathcal{A})$, as long as it can generate a ciphertext ct which differs from all challenge ciphertexts it obtain from the challenge oracle and that $\text{aDec}(\text{sk}, \text{dk}, \text{ct}) \neq \perp$. According to the ROB-CT+ security of AME , this happens only with negligible probability, and hence the sk-dualCCA security of AME holds. $\square$

5.3 Security against the Anamorphic Sender

In this subsection, we investigate the security against the anamorphic sender in the CCA setting. Informally, the anamorphic sender—who holds the double key but not the secret key—is given access to two decryption oracles: a normal decryption and an anamorphic decryption oracle. Security against the anamorphic sender requires that the confidentiality of the normal message, the anamorphic, or potentially both, be preserved against such an adversary.

Definition 8 (dk-CCA-AM Security of AME). *An AME scheme $\text{AME} = (\Pi, \Sigma)$ is dk-CCA-AM-secure, if, for every PPT adversary $\mathcal{A}$, the advantage*

$$\text{Adv}_{\Pi, \Sigma}^{\text{dk-cca-am}}(\mathcal{A}) := |\Pr[\text{dk-CCA-AM}_{\Pi, \Sigma, 1}(\mathcal{A}) = 1] - \Pr[\text{dk-CCA-AM}_{\Pi, \Sigma, 0}(\mathcal{A}) = 1]|$$

is negligible in λ , where the experiment $\text{dk-CCA-AM}_{\Pi, \Sigma, b}(\mathcal{A})$ for $b \in \{0, 1\}$ is defined in Fig. 8.

dk-CCA-AM $_{\Pi, \Sigma, b}(\mathcal{A})$:	CHAL(m_0, m_1)
1 : $(pk, sk, dk) \leftarrow \text{aKGen}(1^\lambda)$	1 : if $(ct^* \neq \perp) \vee (m_0 \neq m_1)$:
2 : $ct^* \leftarrow \perp$	2 : return $\perp$
3 : return $\mathcal{A}^{\text{CHAL, DEC, ADEC}}(pk, dk)$	3 : $ct^* \leftarrow \text{Enc}(pk, m_b)$
	4 : return ct^*
DEC(ct)	ADEC(ct)
1 : if $ct = ct^*$: return $\perp$	1 : return $\text{aDec}(sk, dk, ct)$
2 : return $\text{Dec}(sk, ct)$	

Fig. 8. dk-CCA-AM security game for AME scheme $\text{AME} = (\Pi, \Sigma)$.

Definition 9 (dk-aCCA+ Security of AME). *An AME scheme $\text{AME} = (\Pi, \Sigma)$ is dk-aCCA+-secure, if, for every PPT adversary $\mathcal{A}$, the advantage*

$$\text{Adv}_{\Pi, \Sigma}^{\text{dk-acca+}}(\mathcal{A}) := |\Pr[\text{dk-aCCA+}_{\Pi, \Sigma, 1}(\mathcal{A}) = 1] - \Pr[\text{dk-aCCA+}_{\Pi, \Sigma, 0}(\mathcal{A}) = 1]|$$

is negligible in λ , where the experiment $\text{dk-aCCA+}_{\Pi, \Sigma, b}(\mathcal{A})$ for $b \in \{0, 1\}$ is defined in Fig. 9.

5.4 Randomness-Recovering PKE: Achieving All Symmetric Security Notions

Given the relationships we have established among all security notions (cf. Fig. 1), an AME scheme is most secure if it achieves sk-dualCCA, dk-CCA-AM, and dk-aCCA+ security simultaneously. In this subsection we review the generic

dk-aCCA+ $_{\Pi, \Sigma, b}(\mathcal{A})$:	CHAL($m_0, m_1, \hat{m}_0, \hat{m}_1$)
1 : $(pk, sk, dk) \leftarrow \text{aKGen}(1^\lambda)$	1 : if $(ct^* \neq \perp) \vee (m_0 \neq m_1)$
2 : $ct^* \leftarrow \perp$	$\vee (\hat{m}_0 \neq \hat{m}_1)$:
3 : return $\mathcal{A}^{\text{CHAL}, \text{DEC}, \text{ADec}}(pk, dk)$	2 : return $\perp$
DEC(ct)	3 : $ct^* \leftarrow \text{aEnc}(pk, dk, m_b, \hat{m}_b)$
1 : if $ct = ct^*$: return $\perp$	4 : return ct^*
2 : return Dec(sk, ct)	ADec(ct)
	1 : if $ct = ct^*$: return $\perp$
	2 : return aDec(sk, dk, ct)

Fig. 9. dk-aCCA+ security game for AME scheme $\text{AME} = (\Pi, \Sigma)$.

compiler of AME from randomness-recovering PKE (rr-PKE) schemes [20], and show that under a stronger assumption on the underlying PKE scheme and symmetric encryption scheme, the rr-PKE compiler can achieve all of these security notions.

Definition 10 (Randomness Recovering PKE [20]). A PKE scheme $\Pi = (\text{KGen}, \text{Enc}, \text{Dec})$ is randomness recovering (rr-PKE), if there is a randomness recovering PPT decryption algorithm rrDec such that $\text{rrDec}(sk, ct) = (m, r)$, where $(pk, sk) \leftarrow \text{KGen}(1^\lambda)$, and $ct := \text{Enc}(pk, m; r)$.

The idea of the AME compiler from rr-PKE in [20] is to embed the anamorphic message into the randomness r used in the encryption. More precisely, let Π be an IND-CPA-secure PKE scheme, and SE be an PR-CT-secure symmetric encryption scheme. In the anamorphic triplet Σ , the public key pk and the secret key sk are generated as in Π , and the double key dk is a secret key of SE. The anamorphic encryption algorithm, given a normal message m and an anamorphic message $\hat{m}$, returns the ciphertext $ct := \text{Enc}(pk, m; r)$, where $r \leftarrow \text{SE.Enc}(dk, \hat{m})$. The anamorphic decryption, given a ciphertext ct , first invokes the randomness-recovering decryption algorithm to obtain $\text{rrDec}(sk, ct) = (m, r)$, and then decrypts r using dk to obtain $\text{SE.Dec}(dk, r) = \hat{m}$. For security, [20] proved that PR-CT security of SE directly implies sk-dualCPA security of $\text{AME} = (\Pi, \Sigma)$.

Now we consider to enhance this generic compiler to the CCA setting. It may seem that we are done if the security properties of the underlying PKE and SE schemes are enhanced from CPA to CCA. However, we argue that it is not sk-dualCCA-secure and dk-aCCA+-secure yet, for the following reasons.

1. **Anamorphic decryption oracle.** Given a challenge ciphertext $ct^* = \text{Enc}(pk, m; r)$ where r is either true randomness (in the normal mode) or a symmetric encryption of $\text{SE.Enc}(dk, \hat{m})$ (in the anamorphic mode), the adversary can first decrypt ct^* to obtain the randomness r , and then reuse this r to

encrypt another message $m' \neq m$ to obtain a ciphertext $ct' = \text{Enc}(pk, m'; r)$. Therefore, with the result of $\text{aDec}(sk, dk, ct')$ from anamorphic decryption, which, in the normal mode is $\perp$ and in the anamorphic mode is $\hat{m}$, the adversary is able to distinguish the two modes, and $sk\text{-dualCCA}$ does not hold at all.

2. **Leakage from the double key.** To prove $dk\text{-aCCA}+$ security, we need to argue that an anamorphic encryption of $(m_0, \hat{m}_0)$ is indistinguishable from an anamorphic encryption of $(m_1, \hat{m}_1)$. Namely, $\text{Enc}(pk, m_0; r_0)$ with $r_0 \leftarrow \text{SE.Enc}(dk, \hat{m}_0)$ is indistinguishable from $\text{Enc}(pk, m_1; r_1)$ with $r_1 \leftarrow \text{SE.Enc}(dk, \hat{m}_1)$. It seems that this relies on the IND-CCA security of the underlying PKE scheme. However, to apply IND-CCA property of Π to switch the challenge ciphertext from $\text{Enc}(pk, m_0; r_0)$ to $\text{Enc}(pk, m_1; r_1)$, the randomness (in both encryptions) is required to be fresh. Since the double key dk is known to the adversary, the randomness, which is fixed to be a SE ciphertext in anamorphic encryption, does not provide any freshness at all, causing the reduction from the $dk\text{-aCCA}+$ security of AME to the IND-CPA security of PKE to fail.

We propose some novel methods to solve these problems.

1. To solve the first problem caused by the anamorphic decryption oracle, we replace SE with an authenticated encryption scheme AE,¹¹ and modify the scheme such that the randomness r is a symmetric encryption of both m and $\hat{m}$, i.e., $r \leftarrow \text{AE.Enc}(dk, (m || \hat{m}))$. Meanwhile, in anamorphic decryption w.r.t. a ciphertext $ct = \text{Enc}(pk, m; r)$, it returns $\perp$ directly if $\text{AE.Dec}(dk, r) = (m', \hat{m})$ and $m' \neq m$. Now the adversary who does not know dk can neither generate a randomness that did not decrypt to the failure indicator (the security of AE), nor reuse the randomness r to obtain a different ciphertext, since the ciphertext is uniquely determined by pk , m , and r , and m is fixed once r is determined in the anamorphic encryption mode.
2. To solve the second problem caused by the imperfect randomness due to the leakage of dk , we build an underlying authenticated encryption from IC, and put additional randomness $\hat{r}$ in the encryption. Therefore, even if dk (i.e., the secret key of the symmetric encryption) and the plaintext are known to the adversary, it still cannot predicate $r := \text{IC}_{dk}(m, \hat{m}, \hat{r})$, which is randomly sampled from the output space of IC (i.e., the randomness space of the PKE scheme Π). Consequently, the IND-CCA security of Π is sufficient to prove the $dk\text{-aCCA}+$ security of AME.

As we discussed above, we need an authenticated encryption scheme based on an ideal cipher. One of the simplest approaches to achieve this is following the Encode-then-Encipher (EtE) paradigm [6]. We note that EtE requires that the maximum message length of EtE be smaller than the input message length

¹¹ The concurrent work by Jaeger and Stracovsky [17] mentioned the use of authentication encryption (referred as randomness replacement in [17]) for robustness, but in the syntax of anamorphic signatures.

of the inner ideal cipher. To extend the input domain, one may introduce more *generic* authenticated encryption mode that supports arbitrary length messages with a security proof in the ideal cipher model such as Galois Counter-Mode (GCM) scheme [15] or indifferentiable authenticated encryption [2]. Another way of addressing the length issue is assuming a stronger primitive instead of an ideal cipher, e.g., an ideal *accordion cipher mode* [11], or, in short, an accordion mode.¹² Nonetheless, in this work we stick to the simpler case, which is enough to show feasibility: applying EtE to an ideal cipher.

Let $\text{IC} : \{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ be an ideal cipher and $n = n_1 + n_2 + \lambda_1 + \lambda_2$. The authenticated encryption scheme AE with plaintext space $\{0, 1\}^{n_1 + n_2}$ is constructed as follows.

- $\text{AE.KGen}(1^\lambda)$: The key generation algorithm returns a key dk randomly sampled from $\{0, 1\}^k$.
- $\text{AE.Enc}(\text{dk}, (\text{m} || \hat{\text{m}}))$: The encryption algorithm samples a random string $\hat{r} \leftarrow \{0, 1\}^{\lambda_1}$, and returns $r := \text{IC.Enc}(\text{dk}, (\text{m} || \hat{\text{m}} || \hat{r} || 10^{\lambda_2 - 1}))$.
- $\text{AE.Dec}(\text{dk}, r)$: The decryption algorithm first invokes $\text{IC.Dec}(\text{dk}, r)$ to get $(\text{m}' || \hat{\text{m}}' || \hat{r}' || \mu)$. If $\mu = 10^{\lambda_2 - 1}$, it returns $(\text{m}', \hat{\text{m}}')$. Otherwise, it returns $\perp$.

Now we are ready to describe the compiler of secure AME schemes from rr-PKE. Let $\Pi = (\text{KGen}, \text{Enc}, \text{Dec})$ be a CCA-secure rr-PKE scheme, and AE be an authenticated encryption scheme from ideal cipher IC constructed as above, we design the anamorphic triplet Σ as follows:

- The anamorphic key generation algorithm $\text{aKGen}(1^\lambda)$ returns $(\text{pk}, \text{sk}, \text{dk})$, where $(\text{pk}, \text{sk}) \leftarrow \Pi.\text{KGen}(1^\lambda)$, and $\text{dk} \leftarrow \text{AE.KGen}(1^\lambda)$.
- The anamorphic encryption algorithm $\text{aEnc}(\text{pk}, \text{dk}, \text{m}, \hat{\text{m}})$ returns $\text{ct} := \Pi.\text{Enc}(\text{pk}, \text{m}; r)$, where $r \leftarrow \text{AE.Enc}(\text{dk}, (\text{m} || \hat{\text{m}}))$.
- The anamorphic decryption algorithm $\text{aDec}(\text{pk}, \text{dk}, \text{ct})$ first invokes the randomness recovering algorithm to get $\text{rrDec}(\text{sk}, \text{ct}) = (\text{m}, r)$, and runs $\text{AE.Dec}(\text{dk}, r)$ to obtain $(\text{m}', \hat{\text{m}}')$, and then it returns $\hat{\text{m}}$ if $\text{m} = \text{m}'$ and $\perp$ otherwise (including the case AE.Dec returns $\perp$).

The correctness of Σ follows directly the correctness of Π and AE.

Theorem 6 (Security of AME). *If Π is a CCA-secure rr-PKE scheme, IC is an ideal cipher and AE is a secure AE scheme constructed from IC as above, then the AME scheme $\text{AME} = (\Pi, \Sigma)$ with the anamorphic triplet described above has sk-dualCCA security, dk-CCA-AM security, and dk-aCCA+ security.*

¹² Accordion mode is a relatively new primitive, an ongoing proposal of NIST at the time of writing. We can see it as a variable-length extension of an ideal cipher, which could plausibly be a construction based on an ideal cipher. Therefore, it could be an equivalent assumption to the random oracle model or the ideal cipher model [12, 16] in a single-stage game setting [26]. By assuming an ideal accordion mode, EtE based on the accordion mode naturally supports an arbitrary length input. We believe this will be an interesting model in the near future if accordion mode becomes popular.

Proof. We first prove the sk-dualCCA security of AME. To prove the indistinguishability of the experiment $\text{sk-dualCCA}_{\Pi,\Sigma,1}(\mathcal{A})$ (the anamorphic mode) from the experiment $\text{sk-dualCCA}_{\Pi,\Sigma,0}(\mathcal{A})$ (the normal mode), we introduce a hybrid game $\text{Hybrid}_{\Pi,\Sigma}(\mathcal{A})$ which is the same as $\text{sk-dualCCA}_{\Pi,\Sigma,1}(\mathcal{A})$, except that all anamorphic decryption queries from $\mathcal{A}$ output failure indicator $\perp$.

We analyze the difference between $\text{sk-dualCCA}_{\Pi,\Sigma,1}(\mathcal{A})$ and $\text{Hybrid}_{\Pi,\Sigma}(\mathcal{A})$ as follows. Let $(\mathbf{m}^*, \hat{\mathbf{m}}^*)$ be the challenge query by $\mathcal{A}$, and $\text{ct}^* := \Pi.\text{Enc}(\text{pk}, \mathbf{m}^*; r^*)$ be the challenge ciphertext, where $r^* \leftarrow \text{AE}.\text{Enc}(\text{dk}, (\mathbf{m}^* || \hat{\mathbf{m}}^*))$. If the adversary $\mathcal{A}$ queries a ciphertext $\text{ct} \neq \text{ct}^*$ such that $\text{aDec}(\text{dk}, \text{ct}) \neq \perp$, then $\mathcal{A}$ is able to distinguish $\text{sk-dualCCA}_{\Pi,\Sigma,1}(\mathcal{A})$ from $\text{Hybrid}_{\Pi,\Sigma}(\mathcal{A})$. Assume $\text{rrDec}(\text{sk}, \text{ct}) = (\mathbf{m}, r)$, we further discuss in the following cases.

- Case 1. $\mathbf{m} = \mathbf{m}^*$ and $r = r^*$. This implies that $\text{ct} = \text{ct}^*$ and the oracle will return $\perp$ directly.
- Case 2. $\mathbf{m} \neq \mathbf{m}^*$ but $r = r^*$. Since $\text{AE}.\text{Dec}(\text{dk}, r) = (\mathbf{m}^*, \hat{\mathbf{m}}^*)$, the anamorphic decryption oracle will return $\perp$ since $\mathbf{m} \neq \mathbf{m}^*$.
- Case 3. $r \neq r^*$. The anamorphic decryption does not return $\perp$ only if $\text{AE}.\text{Dec}(\text{dk}, r) \neq \perp$, which means that the adversary generates a distinct but valid ciphertext, and hence breaks the security of AE.

Therefore, $\text{sk-dualCCA}_{\Pi,\Sigma,1}(\mathcal{A})$ and $\text{Hybrid}_{\Pi,\Sigma}(\mathcal{A})$ are indistinguishable to the adversary, due to the security of AE.

Then we analyze the difference between $\text{Hybrid}_{\Pi,\Sigma}(\mathcal{A})$ and $\text{sk-dualCCA}_{\Pi,\Sigma,0}(\mathcal{A})$. Now both anamorphic decryption oracles return $\perp$ all the time, and the only difference between these two games is the randomness r used in encryption, which is randomly sampled in $\text{Hybrid}_{\Pi,\Sigma}(\mathcal{A})$, and $r \leftarrow \text{AE}.\text{Enc}(\text{dk}, (\mathbf{m} || \hat{\mathbf{m}}))$ in $\text{sk-dualCCA}_{\Pi,\Sigma,0}(\mathcal{A})$. Due to the security of AE, which is implied by the property of ideal cipher IC, they are indistinguishable to the adversary $\mathcal{A}$. This finishes the proof of sk-dualCCA security of AME.

Next we prove the dk-aCCA+ security, which requires that $\text{Enc}(\text{pk}, \mathbf{m}_0; r_0)$ is indistinguishable to $\text{Enc}(\text{pk}, \mathbf{m}_1; r_1)$ to the adversary $\mathcal{A}$ holding the double key dk , where $r_0 \leftarrow \text{AE}.\text{Enc}(\text{dk}, (\mathbf{m}_0 || \hat{\mathbf{m}}_0))$, and $r_1 \leftarrow \text{AE}.\text{Enc}(\text{dk}, (\mathbf{m}_1 || \hat{\mathbf{m}}_1))$. Recall that dk is independent from (pk, sk) , and for $b \in \{0, 1\}$, $\text{AE}.\text{Enc}(\text{dk}, (\mathbf{m}_b || \hat{\mathbf{m}}_b)) = \text{IC}_{\text{dk}}(\mathbf{m}_b || \hat{\mathbf{m}}_b || \hat{r}_b || 0^{\lambda_2})$, where $\hat{r}_b \in \{0, 1\}^\lambda$ is a random string sampled in the encryption. Let Q_{IC} denote the number of queries to the ideal cipher IC by the adversary. Unless the adversary has queried $\text{IC}.\text{Enc}$ on $(\mathbf{m}_b || \hat{\mathbf{m}}_b || \hat{r}_b || 0^{\lambda_2})$, which happens with probability at most $Q_{\text{IC}} \cdot 2^{-\lambda_1}$, the resulted ciphertext $r_b = \text{IC}_{\text{dk}}(\mathbf{m}_b || \hat{\mathbf{m}}_b || \hat{r}_b || 0^{\lambda_2})$ is a fresh and random string in the ciphertext space (i.e., the randomness space of PKE scheme Π). Then by the CCA security of Π , the experiment $\text{dk-aCPA}+_{\Pi,\Sigma,0}(\mathcal{A})$ is indistinguishable to the experiment $\text{dk-aCPA}+_{\Pi,\Sigma,1}(\mathcal{A})$, completing the proof of dk-aCCA+ security.

Finally, dk-CCA-AM security of AME is directly implied by the CCA security of the underlying PKE scheme, since the symmetric key dk is independent from the public and secret key pair (pk, sk) of the PKE scheme. Taking all together, Theorem 6 holds consequently. $\square$

6 Security of Asymmetric Anamorphic Encryption

In this section we study the security of asymmetric anamorphic encryption (AAME) [25], where the double key is divided into two parts, the sender double key $\mathbf{sdk}$, which is held by the anamorphic sender and used in anamorphic encryption, and the receiver double key $\mathbf{rdk}$, which is held by the receiver and used in anamorphic decryption. Additional results in this setting are provided in Appendix D. We start by formally defining AAME.

Definition 11 (Asymmetric Anamorphic Encryption). *An asymmetric anamorphic encryption (AAME) scheme $\mathbf{AAME}$ is a public-key encryption scheme $\Pi = (\text{KGen}, \text{Enc}, \text{Dec})$ associated with an anamorphic triplet $\Sigma = (\mathbf{aKGen}, \mathbf{aEnc}, \mathbf{aDec})$ and $\mathbf{AAME}$ has two modes: normal mode and anamorphic mode. When running the normal mode, the primitive is identical to Π . When running the anamorphic mode, Π is replaced by Σ where the algorithms are defined as below:*

- $(\mathbf{pk}, \mathbf{sk}, \mathbf{sdk}, \mathbf{rdk}) \leftarrow \mathbf{aKGen}(1^\lambda)$. On input the parameter λ , the anamorphic key generation algorithm outputs a public key $\mathbf{pk}$, a secret key $\mathbf{sk}$, a sender double key $\mathbf{sdk}$, and a receiver double key $\mathbf{rdk}$.
- $\mathbf{ct} \leftarrow \mathbf{aEnc}(\mathbf{pk}, \mathbf{sdk}, \mathbf{m}, \hat{\mathbf{m}})$. On input the public key $\mathbf{pk}$, the sender double key $\mathbf{sdk}$, a normal message $\mathbf{m}$ and an anamorphic message $\hat{\mathbf{m}}$, the anamorphic encryption algorithm outputs an (anamorphic) ciphertext $\mathbf{ct}$.
- $\hat{\mathbf{m}}/\perp \leftarrow \mathbf{aDec}(\mathbf{sk}, \mathbf{rdk}, \mathbf{ct})$. On input the secret key $\mathbf{sk}$, the receiver double key $\mathbf{rdk}$ and a ciphertext $\mathbf{ct}$, the anamorphic decryption algorithm outputs an anamorphic message $\hat{\mathbf{m}}$ or a failure indicator $\perp$.

Correctness of Σ . *For every message $\mathbf{m}$ and anamorphic message $\hat{\mathbf{m}}$, except with negligible probability in λ over the randomness of $\mathbf{aKGen}$ and $\mathbf{aEnc}$, it holds that*

1. $\mathbf{aDec}(\mathbf{sk}, \mathbf{rdk}, \mathbf{ct}) = \hat{\mathbf{m}}$, and
2. $\text{Dec}(\mathbf{sk}, \mathbf{ct}) = \mathbf{m}$,

where $(\mathbf{pk}, \mathbf{sk}, \mathbf{sdk}, \mathbf{rdk}) \leftarrow \mathbf{aKGen}(1^\lambda)$, and $\mathbf{ct} \leftarrow \mathbf{aEnc}(\mathbf{pk}, \mathbf{sdk}, \mathbf{m}, \hat{\mathbf{m}})$.

Remark 10 (On Defining AAME). We decompose the double key into the sender double key $\mathbf{sdk}$ and the receiver double key $\mathbf{rdk}$, as was done by Persiano, Phan, and Yung [25]. This is equivalent to the definition in [8] where the double key in the symmetric setting is decomposed into a double key (held by the sender) as well as a trapdoor key (held by the receiver). For simplicity, one can also imagine that $\mathbf{sdk}$ is implicitly a part of $\mathbf{rdk}$, just like the relationship between the public key and a secret key in classical PKE schemes. However, we avoid formalizing them as double public key and double secret key since $\mathbf{sdk}$ is not public at all! In fact, $\mathbf{sdk}$ should be kept private against the dictator, as otherwise, the use of an anamorphic channel is totally compromised.

Remark 11 (On Correctness of AAME). Prior works [8,25] on AAME focused solely on the correctness of anamorphic encryption, while neglecting the correctness of normal decryption applied to anamorphic ciphertexts (cf. the second property of correctness above). Similar to the symmetric setting, our definition captures both the correctness of anamorphic decryption and the correctness of normal decryption.

Since most security notions we consider are analogous to those in the symmetric setting, we mainly focus here on the security against the collusion of the dictator and the anamorphic sender, and defer the others to Appendix D.

6.1 Security against the Collusion of the Dictator and the Anamorphic Sender in the Asymmetric Setting

We define sk-sdk-dualCPA and sk-sdk-aCPAa in the CPA setting, and sk-sdk-dualCCA and sk-sdk-aCCAa in the CCA setting as follows.

Definition 12 (sk-sdk-dualCPA/sk-sdk-dualCCA Security of Asymmetric AME). An AAME scheme $\text{AAME} = (\Pi, \Sigma)$ is sk-sdk-dualX-secure for $X \in \{\text{CPA}, \text{CCA}\}$, if, for every PPT adversary $\mathcal{A}$, the advantage

$$\text{Adv}_{\Pi, \Sigma}^{\text{sk-sdk-dualX}}(\mathcal{A}) := |\Pr[\text{sk-sdk-dualX}_{\Pi, \Sigma, 1}(\mathcal{A}) = 1] - \Pr[\text{sk-sdk-dualX}_{\Pi, \Sigma, 0}(\mathcal{A}) = 1]|$$

is negligible in λ , where the experiment $\text{sk-sdk-dualX}_{\Pi, \Sigma, b}(\mathcal{A})$ for $b \in \{0, 1\}$ is defined in Fig. 10.

sk-sdk-dualX _{Π,Σ,b} ($\mathcal{A}$):	CHAL($m, \hat{m}$)
1 : $(pk, sk, sdk, rdk) \leftarrow \text{aKGen}(1^\lambda)$	1 : if $ct^* \neq \perp$: return $\perp$
2 : $ct^* \leftarrow \perp$	2 : if $b = 0$:
3 : return $\mathcal{A}^{\text{CHAL}}(pk, sk, sdk)$	3 : $ct^* \leftarrow \text{Enc}(pk, m)$
4 : return $\mathcal{A}^{\text{CHAL}, \text{ADEC}}(pk, sk, sdk)$	4 : else :
	5 : $ct^* \leftarrow \text{aEnc}(pk, sdk, m, \hat{m})$
	6 : return ct^*
	ADEC(ct)
	1 : if $ct = ct^*$: return $\perp$
	2 : return $\text{aDec}(sk, rdk, ct)$

Fig. 10. sk-sdk-dualX security game for asymmetric AME scheme $\text{AAME} = (\Pi, \Sigma)$ for $X \in \{\text{CPA}, \text{CCA}\}$. Boxed code is only relevant in the sk-sdk-dualCPA game. Highlighted code is only relevant in the sk-sdk-dualCCA game.

Remark 12. Note that the above two security notions are applicable only in the asymmetric setting. In the symmetric setting, $\text{sdk} = \text{rdk}(= \text{dk})$, and both the normal message and the anamorphic message are compromised with the knowledge of sk and dk .

6.2 AAME Schemes Satisfying All Asymmetric Security Notions

In this subsection we modify the generic compiler from rr-PKE in Section 5.4 to the asymmetric setting, and describe how to additionally achieve sk-sdk-dualCCA security. The high-level idea is to replace the authenticated encryption scheme (which encrypts the anamorphic message into “randomness” used in the PKE scheme) with a PKE scheme Π' , so that the double key can be split into two parts, the public key sdk of Π' that is used in anamorphic encryption, and the secret key rdk of Π' that is used in anamorphic decryption. To guarantee that such a replacement will not sacrifice the security of AME, Π' is required to hold both the CCA security and ciphertext pseudorandomness, see Def. 16 for the details.

More precisely, let Π be an IND-CCA-secure rr-PKE scheme, and Π' be a PR-CCA-secure PKE scheme (cf. Def. 16),¹³ we design the anamorphic triplet Σ associated with Π as follows:

- The anamorphic key generation algorithm $\text{aKGen}(1^\lambda)$ returns $(\text{pk}, \text{sk}, \text{sdk}, \text{rdk})$, where $(\text{pk}, \text{sk}) \leftarrow \Pi.\text{KGen}(1^\lambda)$, and $(\text{sdk}, \text{rdk}) \leftarrow \Pi'.\text{KGen}(1^\lambda)$.
- The anamorphic encryption algorithm $\text{aEnc}(\text{pk}, \text{sdk}, \text{m}, \hat{\text{m}})$ returns $\text{ct} := \Pi.\text{Enc}(\text{pk}, \text{m}; r)$, where $r \leftarrow \Pi'.\text{Enc}(\text{sdk}, (\text{m} \parallel \hat{\text{m}}))$.
- The anamorphic decryption algorithm $\text{aDec}(\text{pk}, \text{rdk}, \text{ct})$ first invokes the randomness recovering algorithm to get $\text{rrDec}(\text{sk}, \text{ct}) = (\text{m}, r)$, and runs $\Pi'.\text{Dec}(\text{rdk}, r)$ to obtain $(\text{m}', \hat{\text{m}})$, and then it returns $\hat{\text{m}}$ if $\text{m} = \text{m}'$ and $\perp$ otherwise (including the case $\Pi'.\text{Dec}$ returns $\perp$).

The correctness of Σ follows directly the correctness of Π and AE.

Remark 13 (The underlying SE scheme: AE security v.s. CCA security). In Sec. 5.4, we argue that in the rr-PKE paradigm, the CCA security of the underlying symmetric encryption scheme is insufficient for sk-dualCCA security, and we have to resort to an AE scheme. However, in the asymmetric setting, CCA security and ciphertext pseudorandomness are sufficient. This results from the difference between sk-dualCCA security in the symmetric setting (cf. Def. 7) and sk-sdk-dualCCA security in the asymmetric setting (cf. Def. 12). In sk-dualCCA security, the goal of the adversary is to distinguish the normal mode from the anamorphic mode. Since anamorphic decryption always returns $\perp$ in

¹³ PR-CCA-secure PKE schemes can be constructed from a variety of assumptions, e.g., the oracle Diffie-Hellman assumption [23], and the Matrix-DDH assumption [7, 14, 21], and the Modular-LWE assumption [22].

the normal mode, the adversary wins as long as it can generate a valid anamorphic ciphertext—equivalently—a valid and fresh ciphertext of the underlying SE scheme. Therefore, a CCA-secure SE scheme is insufficient and a stronger AE scheme is required. While in sk-sdk-dualCCA security, the adversary already knows the scheme is working in the anamorphic mode from sdk (the public key of Π'), and its attacking goal is to tell if a *specific* ciphertext is a normal one or an anamorphic one. Therefore, the CCA security of the underlying PKE scheme Π' is sufficient for the sk-sdk-dualCCA security.

Theorem 7 (Security of AAME). *If PKE scheme Π is IND-CCA-secure and randomness recovering, PKE scheme Π' is PR-CCA secure, then the AAME scheme $\text{AAME} = (\Pi, \Sigma)$ with the anamorphic triplet described above has sk-sdk-dualCCA security, dk-CCA-AM security, and dk-aCCA+ security.*

Proof. To prove the sk-sdk-dualCCA security of AAME, it is sufficient to argue that the adversary, given sdk (the public key of Π') and an anamorphic decryption oracle (the decryption oracle of Π') but not rdk (the secret key of Π'), it still cannot tell an encryption of $(\mathbf{m}, \hat{\mathbf{m}})$ from a random string of the same length of the ciphertext. We then construct a reduction algorithm $\mathcal{A}'$ to show that, if $\mathcal{A}$ can distinguish the experiment $\text{sk-sdk-dualCCA}_{\Pi, \Sigma, 1}(\mathcal{A})$ (the anamorphic mode) from the experiment $\text{sk-sdk-dualCCA}_{\Pi, \Sigma, 0}(\mathcal{A})$ (the normal mode), then $\mathcal{A}'$ is able to break the PR-CCA security of Π' .

$\mathcal{A}'$ simulates the experiment to $\mathcal{A}$ as follows.

- $\mathcal{A}'$ receives the public key sdk of Π' from its own challenger. It generates $(\text{pk}, \text{sk}) \leftarrow \Pi.\text{KGen}(1^\lambda)$, and passes $(\text{pk}, \text{sk}, \text{sdk})$ to $\mathcal{A}$.
- When $\mathcal{A}$ asks a challenge query $(\mathbf{m}^*, \hat{\mathbf{m}}^*)$, the reduction algorithm $\mathcal{A}'$ queries $(\mathbf{m}^*, \hat{\mathbf{m}}^*)$ to its own challenger and obtains r^* , which is either a random string or an encryption $\Pi.\text{Enc}(\text{sdk}, (\mathbf{m}^*, \hat{\mathbf{m}}^*))$. Then $\mathcal{A}'$ uses this r as the randomness to generate $\text{ct}^* := \Pi.\text{Enc}(\text{pk}, \mathbf{m}^*; r^*)$ and passes ct^* as the ciphertext to $\mathcal{A}$.
- When $\mathcal{A}$ asks an anamorphic decryption query with $\text{ct} \neq \text{ct}^*$, $\mathcal{A}'$ first invokes $\Pi.\text{rrDec}(\text{sk}, \text{ct}) = (\mathbf{m}, r)$. If the decryption fails or $r = r^*$ then $\mathcal{A}'$ returns $\perp$ directly. Otherwise, $\mathcal{A}'$ queries its decryption oracle with input r and obtains the result. If the decryption result is $(\mathbf{m}', \hat{\mathbf{m}}')$ such that $\mathbf{m}' \neq \mathbf{m}$, then $\mathcal{A}'$ returns $\mathbf{m}'$ to $\mathcal{A}$; in all other cases, $\mathcal{A}'$ returns $\perp$.

We now analyze the simulation by $\mathcal{A}'$. Recall that in the experiment $\text{sk-sdk-dualCCA}_{\Pi, \Sigma, 1}(\mathcal{A})$, the adversary $\mathcal{A}$ is not allowed to ask an anamorphic query with the challenge ciphertext. Since the challenge ciphertext (of Π) is totally determined by the message and the randomness, it is impossible to provide a ciphertext $\text{ct} \neq \text{ct}^*$ such that $\text{rrDec} = (\mathbf{m}, r) = (\mathbf{m}^*, r^*)$. If $r = r^*$ but $\mathbf{m} \neq \mathbf{m}^*$, which means that $\mathcal{A}$ reused r^* to encrypt a distinct message $\mathbf{m}$, then $\mathcal{A}'$ directly returns $\perp$ since r^* is either a random string or an encryption of $(\mathbf{m}^*, \cdot)$ so that with negligible probability r^* can be decrypted to $(\mathbf{m}, \cdot)$.

Therefore, if $\mathcal{A}'$ has access to $\text{PR-CCA}_{\Pi', 1}(\mathcal{A}')$ (where r^* is a random string), then $\mathcal{A}'$ simulates $\text{sk-sdk-dualCCA}_{\Pi, \Sigma, 0}(\mathcal{A})$ for $\mathcal{A}$, and if $\mathcal{A}'$ has ac-

cess to $\text{PR-CT}_{\Pi',0}(\mathcal{A}')$ (where r^* is an encryption), then $\mathcal{A}'$ simulates $\text{sk-sdk-dualCCA}_{\Pi,\Sigma,1}(\mathcal{A})$ for $\mathcal{A}$. By the PR-CCA security of Π' , sk-sdk-dualCCA security of AAME is achieved.

Next we prove the sdk-aCCA+ security, which requires that $\text{Enc}(\text{pk}, \text{m}_0; r_0)$ is indistinguishable to $\text{Enc}(\text{pk}, \text{m}_1; r_1)$ to the adversary $\mathcal{A}$ holding both sk and sdk , where $r_0 \leftarrow \Pi'.\text{Enc}(\text{sdk}, (\text{m}_0 || \hat{\text{m}}_0))$, and $r_1 \leftarrow \Pi'.\text{Enc}(\text{dk}, (\text{m}_1 || \hat{\text{m}}_1))$. Recall that (sdk, rdk) is independent from (pk, sk) . By the PR-CCA security of Π' , given sdk , the encryption $(\text{m}_0 || \hat{\text{m}}_0)$ (resp., $(\text{m}_1 || \hat{\text{m}}_1)$) is indistinguishable from a random string. Then, given r_0 (resp., r_1) to be fresh and random string, sdk-aCCA+ of AAME is implied by the IND-CCA security of Π .

Finally, the dk-CCA-AM security of AAME is directly implied by the IND-CCA security of the underlying PKE scheme Π' . This concludes the proof. $\square$

Acknowledgements. We would like to thank the anonymous reviewers of EUROCRYPT 2025 for their insightful feedback, and Roy Stracovsky for the very valuable discussions, especially for pointing out the counter-example in the proof of Theorem 2. The authors were supported in part by AnalytiXIN and by Sunday Group, Inc.

References

1. Banfi, F., Gegier, K., Hirt, M., Maurer, U., Rito, G.: Anamorphic encryption, revisited. In: Advances in Cryptology - EUROCRYPT 2024. vol. 14652, pp. 3–32. Springer (2024). https://doi.org/10.1007/978-3-031-58723-8_1, https://doi.org/10.1007/978-3-031-58723-8_1
2. Barbosa, M., Farshim, P.: Indifferentiable authenticated encryption. In: Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part I. vol. 10991, pp. 187–220. Springer (2018). https://doi.org/10.1007/978-3-319-96884-1_7, https://doi.org/10.1007/978-3-319-96884-1_7
3. Bellare, M., Desai, A., Pointcheval, D., Rogaway, P.: Relations among notions of security for public-key encryption schemes. In: Advances in Cryptology—CRYPTO’98. pp. 26–45. Springer (1998)
4. Bellare, M., Hoang, V.T., Rogaway, P.: Foundations of garbled circuits. In: Proceedings of the 2012 ACM conference on Computer and communications security. pp. 784–796 (2012)
5. Bellare, M., Namprempre, C.: Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. Journal of cryptology **21**(4), 469–491 (2008)
6. Bellare, M., Rogaway, P.: Encode-then-encipher encryption: How to exploit nonces or redundancy in plaintexts for efficient cryptography. In: ASIACRYPT 2000. vol. 1976, pp. 317–330. Springer (2000). https://doi.org/10.1007/3-540-44448-3_24, https://doi.org/10.1007/3-540-44448-3_24
7. Blazy, O., Kiltz, E., Pan, J.: (hierarchical) identity-based encryption from affine message authentication. In: Advances in Cryptology—CRYPTO 2014. pp. 408–425. Springer (2014)

8. Catalano, D., Giunta, E., Migliaro, F.: Anamorphic encryption: New constructions and homomorphic realizations. In: *Advances in Cryptology - EURO-CRYPT 2024*. vol. 14652, pp. 33–62. Springer (2024). https://doi.org/10.1007/978-3-031-58723-8_2, https://doi.org/10.1007/978-3-031-58723-8_2
9. Catalano, D., Giunta, E., Migliaro, F.: Generic anamorphic encryption, revisited: New limitations and constructions. *Cryptology ePrint Archive* (2024)
10. Catalano, D., Giunta, E., Migliaro, F.: Limits of black-box anamorphic encryption. In: *Advances in Cryptology - CRYPTO 2024*. vol. 14921, pp. 352–383. Springer (2024). https://doi.org/10.1007/978-3-031-68379-4_11, https://doi.org/10.1007/978-3-031-68379-4_11
11. Chen, Y.L., Davidson, M., Dworkin, M., Kang, J., Kelsey, J., Sasaki, Y., Turan, M.S., Chang, D., Mouha, N., Largo, M., et al.: Proposal of requirements for an accordion mode. In: *Discussion Draft for the NIST Accordion Mode Workshop 2024* (2024)
12. Coron, J., Patarin, J., Seurin, Y.: The random oracle model and the ideal cipher model are equivalent. In: *CRYPTO 2008*. vol. 5157, pp. 1–20. Springer (2008). https://doi.org/10.1007/978-3-540-85174-5_1, https://doi.org/10.1007/978-3-540-85174-5_1
13. Froomkin, A.M.: Metaphor is the key: cryptography, the clipper chip, and the constitution. *U. Pa. L. Rev.* **143**, 709 (1994)
14. Han, S., Liu, S., Qin, B., Gu, D.: Tightly cca-secure identity-based encryption with ciphertext pseudorandomness. *Designs, Codes and Cryptography* **86**, 517–554 (2018)
15. Hoang, V.T., Tessaro, S., Thiruvengadam, A.: The multi-user security of gcm, revisited: Tight bounds for nonce randomization. In: *CCS 2018*. pp. 1429–1440. ACM (2018). <https://doi.org/10.1145/3243734.3243816>, <https://doi.org/10.1145/3243734.3243816>
16. Holenstein, T., Künzler, R., Tessaro, S.: Equivalence of the random oracle model and the ideal cipher model, revisited. *CoRR* **abs/1011.1264** (2010), <http://arxiv.org/abs/1011.1264>
17. Jaeger, J., Stracovsky, R.: Dictators? friends? forgers. In: *International Conference on the Theory and Application of Cryptology and Information Security*. pp. 105–137. Springer (2024)
18. Koppula, V., Waters, B.: Realizing chosen ciphertext security generically in attribute-based encryption and predicate encryption. In: *Advances in Cryptology - CRYPTO 2019*. vol. 11693, pp. 671–700. Springer (2019). https://doi.org/10.1007/978-3-030-26951-7_23, https://doi.org/10.1007/978-3-030-26951-7_23
19. Kutyłowski, M., Persiano, G., Phan, D.H., Yung, M., Zawada, M.: Anamorphic signatures: Secrecy from a dictator who only permits authentication! In: *Annual International Cryptology Conference*. pp. 759–790. Springer (2023)
20. Kutyłowski, M., Persiano, G., Phan, D.H., Yung, M., Zawada, M.: The self-anti-censorship nature of encryption: On the prevalence of anamorphic cryptography. *Proc. Priv. Enhancing Technol.* **2023**(4), 170–183 (2023). <https://doi.org/10.56553/POPETS-2023-0104>, <https://doi.org/10.56553/popets-2023-0104>
21. Liu, X., Liu, S., Han, S., Gu, D.: Fine-grained verifier nizk and its applications. In: *IACR International Conference on Public-Key Cryptography*. pp. 482–511. Springer (2023)
22. Maram, V., Xagawa, K.: Post-quantum anonymity of kyber. In: *IACR International Conference on Public-Key Cryptography*. pp. 3–35. Springer (2023)

23. Möller, B.: A public-key encryption scheme with pseudo-random ciphertexts. In: Computer Security—ESORICS 2004. pp. 335–351. Springer (2004)
24. Persiano, G., Phan, D.H., Yung, M.: Anamorphic encryption: Private communication against a dictator. In: Advances in Cryptology - EUROCRYPT 2022. vol. 13276, pp. 34–63. Springer (2022). https://doi.org/10.1007/978-3-031-07085-3_2, https://doi.org/10.1007/978-3-031-07085-3_2
25. Persiano, G., Phan, D.H., Yung, M.: Public-key anamorphism in (cca-secure) public-key encryption and beyond. In: Advances in Cryptology - CRYPTO 2024. vol. 14921, pp. 422–455. Springer (2024). https://doi.org/10.1007/978-3-031-68379-4_13, https://doi.org/10.1007/978-3-031-68379-4_13
26. Ristenpart, T., Shacham, H., Shrimpton, T.: Careful with composition: Limitations of the indistinguishability framework. In: EUROCRYPT 2011. vol. 6632, pp. 487–506. Springer (2011). https://doi.org/10.1007/978-3-642-20465-4_27, https://doi.org/10.1007/978-3-642-20465-4_27
27. Shannon, C.E.: Communication theory of secrecy systems. The Bell system technical journal **28**(4), 656–715 (1949)
28. Wang, W., Han, S., Liu, S.: Anamorphic authenticated key exchange: Double key distribution under surveillance. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 168–200. Springer (2025)
29. Wang, Y., Chen, R., Huang, X., Yung, M.: Sender-anamorphic encryption reformulated: Achieving robust and generic constructions. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 135–167. Springer (2023)
30. Woollacott, E.: UK Orders Apple To Open Up Encrypted Messages Worldwide. <https://www.forbes.com/sites/emmawoollacott/2025/02/07/uk-orders-apple-to-open-up-encrypted-messages-worldwide/> (2025)

A Additional Preliminaries

A.1 Public-Key Encryption

Definition 13 (Public-Key Encryption). A public-key encryption (PKE) scheme is a triplet of algorithms $\Pi = (\text{KGen}, \text{Enc}, \text{Dec})$ defined in the following.

- $(\text{sk}, \text{pk}) \leftarrow \text{KGen}(1^\lambda)$. On input the security parameter λ , the key generation algorithm outputs a secret key sk and a public key pk .
- $\text{ct} \leftarrow \text{Enc}(\text{pk}, \text{m})$. On input pk and a message m , the encryption algorithm outputs a ciphertext ct . If the randomness R is specified, we denote as $\text{ct} := \text{Enc}(\text{pk}, \text{m}; R)$.
- $\text{m}/\perp \leftarrow \text{Dec}(\text{sk}, \text{ct})$. On input sk and ct , the decryption algorithm outputs a decryption m or a failure indicator $\perp$.

Correctness of Π . For every message m , except with negligible probability in λ over the randomness of KGen and Enc , it holds that $\text{Dec}(\text{sk}, \text{ct}) = \text{m}$, where $(\text{pk}, \text{sk}) \leftarrow \text{KGen}(1^\lambda)$, and $\text{ct} \leftarrow \text{Enc}(\text{pk}, \text{m})$.

Definition 14 (IND-CPA Security of PKE). A public-key encryption scheme $\Pi = (\text{KGen}, \text{Enc}, \text{Dec})$ is IND-CPA-secure, if, for every PPT adversary $\mathcal{A}$, the advantage

$$\text{Adv}_{\Pi}^{\text{ind-cpa}}(\mathcal{A}) := |\Pr[\text{IND-CPA}_{\Pi,1}(\mathcal{A}) = 1] - \Pr[\text{IND-CPA}_{\Pi,0}(\mathcal{A}) = 1]|$$

is negligible in λ , where the experiment $\text{IND-CPA}_{\Pi,b}(\mathcal{A})$ for $b \in \{0, 1\}$ is defined in Fig. 11.

$\text{IND-CPA}_{\Pi,b}(\mathcal{A})$:	$\text{CHAL}(\text{m}_0, \text{m}_1)$
1 : $(\text{pk}, \text{sk}) \leftarrow \text{KGen}(1^\lambda)$	1 : if $\text{chal} \vee (\text{m}_0 \neq \text{m}_1)$: return $\perp$
2 : $\text{chal} \leftarrow \text{false}$	2 : $\text{chal} \leftarrow \text{true}$
3 : return $\mathcal{A}^{\text{CHAL}}(\text{pk})$	3 : return $\text{Enc}(\text{pk}, \text{m}_b)$

Fig. 11. IND-CPA security game for PKE scheme Π .

Definition 15 (IND-CCA security of PKE). A PKE scheme $\Pi = (\text{KGen}, \text{Enc}, \text{Dec})$ is IND-CCA-secure, if, for every PPT adversary $\mathcal{A}$, the advantage

$$\text{Adv}_{\Pi}^{\text{ind-cca}}(\mathcal{A}) := |\Pr[\text{IND-CCA}_{\Pi,1}(\mathcal{A}) = 1] - \Pr[\text{IND-CCA}_{\Pi,0}(\mathcal{A}) = 1]|$$

is negligible in λ , where the experiment $\text{IND-CCA}_{\Pi,b}(\mathcal{A})$ for $b \in \{0, 1\}$ is defined in Fig. 12.

IND-CCA $_{\Pi,b}(\mathcal{A})$:	CHAL(m_0, m_1)
1 : $(pk, sk) \leftarrow \text{KGen}(1^\lambda)$	1 : if $(ct^* \neq \perp) \vee (m_0 \neq m_1)$: return $\perp$
2 : $ct^* \leftarrow \perp$	2 : $ct^* \leftarrow \text{Enc}(pk, m_b)$
3 : return $\mathcal{A}^{\text{CHAL}, \text{DEC}}(pk)$	3 : return ct^*
	DEC(ct)
	1 : if $ct = ct^*$: return $\perp$
	2 : return $\text{Dec}(sk, ct)$

Fig. 12. IND-CCA security game for PKE scheme Π .

Definition 16 (Ciphertext Pseudorandomness security of PKE). A PKE scheme $\Pi = (\text{KGen}, \text{Enc}, \text{Dec})$ is PR-CCA-secure, if, for every PPT adversary $\mathcal{A}$, the advantage

$$\text{Adv}_{\Pi}^{\text{pr-cca}}(\mathcal{A}) := |\Pr[\text{PR-CCA}_{\Pi,1}(\mathcal{A}) = 1] - \Pr[\text{PR-CCA}_{\Pi,0}(\mathcal{A}) = 1]|$$

is negligible in λ , where the experiment $\text{PR-CCA}_{\Pi,b}(\mathcal{A})$ for $b \in \{0, 1\}$ is defined in Fig. 13.

PR-CCA $_{\Pi,b}(\mathcal{A})$:	ENC(m)
1 : $(pk, sk) \leftarrow \text{KGen}(1^\lambda)$	1 : if $ct^* \neq \perp$: return $\perp$
2 : $ct^* \leftarrow \perp$	2 : $ct^* \leftarrow \text{Enc}(pk, m)$
3 : return $\mathcal{A}^{\text{ENC}, \text{DEC}}(pk)$	3 : if $b = 0$:
	4 : return ct^*
DEC(ct)	5 : else :
1 : if $ct = ct^*$: return $\perp$	6 : return $r \leftarrow_{\$} \mathcal{CT}$
2 : return $\text{Dec}(sk, ct)$	

Fig. 13. PR-CCA security game for PKE scheme Π associated with ciphertext space $\mathcal{CT}$.

PR-CCA-secure PKE schemes can be constructed from a variety of assumptions, e.g., the oracle Diffie-Hellman assumption [23], and the Matrix-DDH assumption [7, 14, 21], and the Modular-LWE assumption [22].

A.2 Symmetric Encryption

Definition 17 (Symmetric Encryption). A (randomized) symmetric encryption (SE) scheme is a triplet of algorithms $\text{SE} = (\text{KGen}, \text{Enc}, \text{Dec})$ defined in the following.

- $k \leftarrow \text{KGen}(1^\lambda)$: On input the security parameter λ , the key generation algorithm outputs a secret key k .
- $ct \leftarrow \text{Enc}(k, m)$: On input k and a message m , the encryption algorithm outputs a ciphertext ct . If the randomness R is specified, we denote as $ct := \text{Enc}(k, m; R)$.
- $m/\perp \text{Dec}(k, ct)$: On input k and ct , the decryption algorithm outputs a message m or a failure indicator $\perp$.

Correctness of SE. For every message m , except with negligible probability over the randomness of KGen and Enc , it holds that $\text{Dec}(k, ct) = m$, where $k \leftarrow \text{KGen}(1^\lambda)$, and $ct \leftarrow \text{Enc}(k, m)$.

Definition 18 (Ciphertext Pseudorandomness (PR-CT) of SE [24,20]). A symmetric encryption scheme $\text{SE} = (\text{KGen}, \text{Enc}, \text{Dec})$ is PR-CT-secure, if, for every PPT adversary $\mathcal{A}$, the advantage

$$\text{Adv}_{\text{SE}}^{\text{pr-ct}}(\mathcal{A}) := |\Pr[\text{PR-CT}_{\text{SE},1}(\mathcal{A}) = 1] - \Pr[\text{PR-CT}_{\text{SE},0}(\mathcal{A}) = 1]|$$

is negligible in λ , where the experiment $\text{PR-CT}_{\text{SE},b}(\mathcal{A})$ for $b \in \{0,1\}$ is defined in Fig. 14.

$\text{PR-CT}_{\text{SE},b}(\mathcal{A})$:	$\text{ENC}(m)$
1: $k \leftarrow \text{KGen}(1^\lambda)$	1: if $ct \neq \perp$: return $\perp$
2: $ct \leftarrow \perp$	2: $ct \leftarrow \text{Enc}(k, m)$
3: return $\mathcal{A}^{\text{ENC}}$	3: if $b = 0$:
	4: return ct
	5: else :
	6: return $r \leftarrow_{\$} \{0,1\}^{ ct }$

Fig. 14. PR-CT security game for SE scheme SE.

A.3 Authenticated Encryption

Definition 19 (Authenticated Encryption). An authenticated encryption (AE) scheme is a particular symmetric encryption scheme $\text{AE} = (\text{KGen}, \text{Enc}, \text{Dec})$ which additionally satisfies the following. For every PPT adversary $\mathcal{A}$, the advantage

$$\text{Adv}_{\text{AE}}^{\text{ae}}(\mathcal{A}) := |\Pr[\text{AE}_{\text{AE},1}(\mathcal{A}) = 1] - \Pr[\text{AE}_{\text{AE},0}(\mathcal{A}) = 1]|$$

is negligible in λ , where the experiment $\text{AE}_{\text{AE},b}(\mathcal{A})$ for $b \in \{0,1\}$ is defined in Fig. 15.

$\text{AE}_{\text{AE},b}(\mathcal{A})$:	$\text{ENC}(m)$	$\text{DEC}(ct)$
1 : $k \leftarrow \text{KGen}(1^\lambda)$	1 : if $b = 0$:	1 : if $b = 0 \wedge ct \notin \mathcal{C}$:
2 : $\mathcal{C} := \emptyset$	2 : $ct \leftarrow \text{Enc}(k, m)$	2 : return $\text{Dec}(k, ct)$
3 : return $\mathcal{A}^{\text{ENC}, \text{DEC}}$	3 : else :	3 : else :
	4 : $ct \leftarrow_{\$} \{0, 1\}^{ \text{Enc}(k, m) }$	4 : return $\perp$
	5 : $\mathcal{C} := \mathcal{C} \cup \{ct\}$	
	6 : return ct	

Fig. 15. Security game for AE scheme AE.

A.4 Pseudorandom Functions

Definition 20 (Pseudorandom Functions). A pseudorandom function (PRF) is a family of functions $\{F_k : \mathcal{X} \rightarrow \mathcal{Y}\}_{k \in \mathcal{K}}$ that satisfy the following properties.

- Given k and $x \in \mathcal{X}$, the computation of $F_k(x)$ is efficient.
- For any PPT adversary $\mathcal{A}$, the advantage

$$\text{Adv}_F^{\text{prf}}(\mathcal{A}) := \left| \Pr[\mathcal{A}^{F_k(\cdot)} = 1] - \Pr[\mathcal{A}^{R(\cdot)} = 1] \right|$$

is negligible in λ , where $k \leftarrow \mathcal{K}$, and R is a random function from $\mathcal{X}$ to $\mathcal{Y}$.

A.5 Ideal Ciphers

An ideal cipher is an idealized model for block ciphers that maps $\{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ for key space $\{0, 1\}^k$, plaintext space $\{0, 1\}^n$, and ciphertext space $\{0, 1\}^n$. An ideal cipher was first defined in Shannon's work [27] as a *random cipher*. Fig. 16 shows the functionality of an ideal cipher (Enc, Dec).

B Additional Results in the CPA Setting

In this section we provide additional security notions for AME, including sk-aCPAa security, dk-aCPAn security, dk-aCPAa security, and present the full structure for the security of AME by investigating relationships among different security notions.

We first prove the following lemma which will be used in other proofs later.

Lemma 1. Let $\text{AME} = (\Pi, \Sigma)$ be an AME scheme. If AME is sk-dualCPA-secure, then, for every PPT adversary $\mathcal{A}$, it holds that

$$\left| \Pr[\text{sk-dualCPA}_{\Pi, \Sigma, 0}(\mathcal{A}) = 1] - \Pr[\text{Hybrid-dualCPA}_{\Pi, \Sigma}(\mathcal{A})] \right| \leq \text{negl}(\lambda),$$

$$\text{and } \left| \Pr[\text{sk-dualCPA}_{\Pi, \Sigma, 1}(\mathcal{A}) = 1] - \Pr[\text{Hybrid-dualCPA}_{\Pi, \Sigma}(\mathcal{A})] \right| \leq \text{negl}(\lambda),$$

where the experiment $\text{sk-dualCPA}_{\Pi, \Sigma, b}(\mathcal{A})$ for $b \in \{0, 1\}$ is defined in Fig. 2, and the experiment $\text{Hybrid-dualCPA}_{\Pi, \Sigma}(\mathcal{A})$ is defined in Fig. 17.

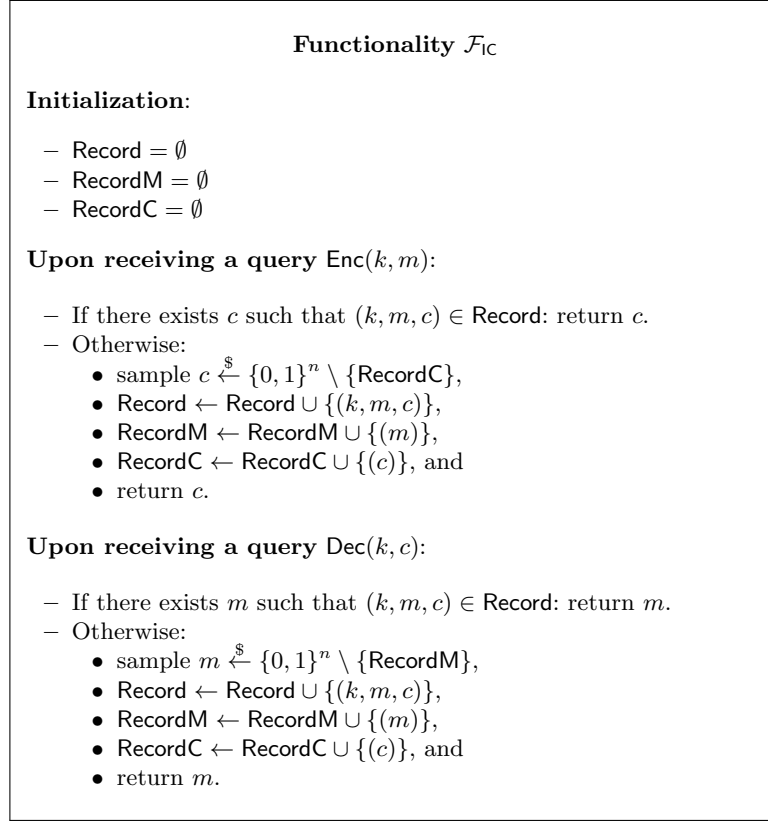


Fig. 16. The functionality $\mathcal{F}_{\text{IC}}$ of an ideal cipher IC.

Proof. We prove the first inequality, and the second inequality holds consequently given AME is sk-dualCPA-secure.

We construct a reduction algorithm $\mathcal{A}'$ to show that, if a PPT adversary $\mathcal{A}$ can distinguish $\text{sk-dualCPA}_{\Pi, \Sigma, 0}(\mathcal{A})$ from $\text{Hybrid-dualCPA}_{\Pi, \Sigma}(\mathcal{A})$, then $\mathcal{A}'$ is able to distinguish $\text{sk-dualCPA}_{\Pi, \Sigma, 0}(\mathcal{A}')$ from $\text{sk-dualCPA}_{\Pi, \Sigma, 1}(\mathcal{A}')$.

$\mathcal{A}'$ simulates the experiment for $\mathcal{A}$ as follows. It first obtains (pk, sk) from the challenger of the experiment $\text{sk-dualCPA}_{\Pi, \Sigma, b}(\mathcal{A}')$ ($b \in \{0, 1\}$), and passes (pk, sk) to $\mathcal{A}$. Whenever $\mathcal{A}'$ receives a challenge query $\text{CHAL}(\text{m}, \hat{\text{m}})$ from $\mathcal{A}$, it returns $\text{Enc}(\text{pk}, \text{m})$. Finally, $\mathcal{A}'$ outputs what $\mathcal{A}$ outputs.

It is easy to see that if $b = 0$, then $\mathcal{A}'$ perfectly simulates the experiment $\text{sk-dualCPA}_{\Pi, \Sigma, 0}(\mathcal{A})$ for $\mathcal{A}$, and if $b = 1$, then $\mathcal{A}'$ perfectly simulates the experiment $\text{Hybrid-dualCPA}_{\Pi, \Sigma}(\mathcal{A})$ for $\mathcal{A}$. Therefore, $\mathcal{A}'$ can distinguish $\text{sk-dualCPA}_{\Pi, \Sigma, 0}(\mathcal{A}')$ from $\text{sk-dualCPA}_{\Pi, \Sigma, 1}(\mathcal{A}')$ as long as $\mathcal{A}$ can distinguish $\text{sk-dualCPA}_{\Pi, \Sigma, 0}(\mathcal{A})$ from $\text{Hybrid-dualCPA}_{\Pi, \Sigma}(\mathcal{A})$, which finishes the proof. $\square$

Hybrid-dualCPA $_{\Pi, \Sigma}(\mathcal{A})$:	CHAL(m, $\hat{m}$)
1 : (pk, sk, dk) $\leftarrow$ aKGen(1^λ)	1 : if chal : return $\perp$
2 : chal $\leftarrow$ false	2 : chal $\leftarrow$ true
3 : return $\mathcal{A}^{\text{CHAL}}(\text{pk}, \text{sk})$	3 : return Enc(pk, m)

Fig. 17. Hybrid-dualCPA security game for AME scheme $\text{AME} = (\Pi, \Sigma)$.

We formalize sk-aCPAa security, which considers the confidentiality of the anamorphic message $\hat{m}$ after anamorphic encryption (against an adversary that has access to (pk, sk) but not dk).

Definition 21 (sk-aCPAa Security of AME [24]). An AME scheme $\text{AME} = (\Pi, \Sigma)$ is sk-aCPAa-secure, if, for every PPT adversary $\mathcal{A}$, the advantage

$$\text{Adv}_{\Sigma}^{\text{sk-acpaa}}(\mathcal{A}) := |\Pr[\text{sk-aCPAa}_{\Sigma,1}(\mathcal{A}) = 1] - \Pr[\text{sk-aCPAa}_{\Sigma,0}(\mathcal{A}) = 1]|$$

is negligible in λ , where the experiment $\text{sk-aCPAa}_{\Sigma,b}(\mathcal{A})$ for $b \in \{0, 1\}$ is defined in Fig. 18.

sk-aCPAa $_{\Sigma,b}(\mathcal{A})$:	CHAL(m, $\hat{m}_0, \hat{m}_1$)
1 : (pk, sk, dk) $\leftarrow$ aKGen(1^λ)	1 : if chal $\vee (\hat{m}_0 \neq \hat{m}_1)$: return $\perp$
2 : chal $\leftarrow$ false	2 : chal $\leftarrow$ true
3 : return $\mathcal{A}^{\text{CHAL, AENC}}(\text{pk}, \text{sk})$	3 : return aEnc(pk, dk, m, $\hat{m}_b$)
	AENC(m, $\hat{m}$)
	1 : return aEnc(pk, dk, m, $\hat{m}$)

Fig. 18. sk-aCPAa security game for AME scheme $\text{AME} = (\Pi, \Sigma)$.

The following relation was proven in [24].

Theorem 8 (sk-dualCPA $\Rightarrow$ sk-aCPAa [24]). Let $\text{AME} = (\Pi, \Sigma)$ be an AME scheme. If AME is sk-dualCPA-secure, then it is also sk-aCPAa-secure.

Proof Sketch. We introduce a hybrid game $\text{Hybrid}_{\Pi, \Sigma, b}(\mathcal{A})$ for $b \in \{0, 1\}$, which is exactly the experiment $\text{sk-aCPAa}_{\Sigma, b}(\mathcal{A})$ except that $(\text{pk}, \text{sk}, \text{dk}) \leftarrow \text{aKGen}(1^\lambda)$ is replaced with $(\text{pk}, \text{sk}) \leftarrow \text{KGen}(1^\lambda)$, and $\text{aEnc}(\text{pk}, \text{dk}, m, \hat{m}_b)$ is replaced with $\text{Enc}(\text{pk}, m_b)$. Thanks to the sk-dualCPA security of (Π, Σ) , $\text{sk-aCPAa}_{\Sigma, b}(\mathcal{A})$ is indistinguishable from $\text{Hybrid}_{\Pi, \Sigma, b}(\mathcal{A})$ for $b \in \{0, 1\}$. Furthermore, $\text{Hybrid}_{\Pi, \Sigma, 0}(\mathcal{A})$ and $\text{Hybrid}_{\Pi, \Sigma, 1}(\mathcal{A})$ are identical to the adversary, since no information of b is leaked at all, which concludes the proof. $\square$

Now we recall the work by Kutyłowski et al. [20], which examined the security against the anamorphic sender,¹⁴ specifically addressing whether the double key is sufficient to read the normal message encrypted in an anamorphic ciphertext.

Definition 22 (dk-aCPAn Security of AME (Single-An Security in [20])). An AME scheme $\text{AME} = (\Pi, \Sigma)$ is dk-aCPAn-secure, if, for every PPT adversary $\mathcal{A}$, the advantage

$$\text{Adv}_{\Sigma}^{\text{dk-acpan}}(\mathcal{A}) := |\Pr[\text{dk-aCPAn}_{\Sigma,1}(\mathcal{A}) = 1] - \Pr[\text{dk-aCPAn}_{\Sigma,0}(\mathcal{A}) = 1]|$$

is negligible in λ , where the experiment $\text{dk-aCPAn}_{\Sigma,b}(\mathcal{A})$ for $b \in \{0, 1\}$ is defined in Fig. 19.

$\text{dk-aCPAn}_{\Sigma,b}(\mathcal{A})$:	$\text{CHAL}(\mathbf{m}_0, \mathbf{m}_1, \hat{\mathbf{m}})$
1 : $(\mathbf{pk}, \mathbf{sk}, \mathbf{dk}) \leftarrow \mathbf{aKGen}(1^\lambda)$	1 : if $\text{chal} \vee (\mathbf{m}_0 \neq \mathbf{m}_1)$: return $\perp$
2 : $\text{chal} \leftarrow \text{false}$	2 : $\text{chal} \leftarrow \text{true}$
3 : return $\mathcal{A}^{\text{CHAL}}(\mathbf{pk}, \mathbf{dk})$	3 : return $\mathbf{aEnc}(\mathbf{pk}, \mathbf{dk}, \mathbf{m}_b, \hat{\mathbf{m}})$

Fig. 19. dk-aCPAn security game for AME scheme $\text{AME} = (\Pi, \Sigma)$.

We consider the analogous notion we introduce for *anamorphic* encryption below.

Definition 23 (dk-aCPAa Security of AME). An AME scheme $\text{AME} = (\Pi, \Sigma)$ is dk-aCPAa-secure, if, for every PPT adversary $\mathcal{A}$, the advantage

$$\text{Adv}_{\Sigma}^{\text{dk-acpaa}}(\mathcal{A}) := |\Pr[\text{dk-aCPAa}_{\Sigma,1}(\mathcal{A}) = 1] - \Pr[\text{dk-aCPAa}_{\Sigma,0}(\mathcal{A}) = 1]|$$

is negligible in λ , where the experiment $\text{dk-aCPAa}_{\Sigma,b}(\mathcal{A})$ for $b \in \{0, 1\}$ is defined in Fig. 4.

It is straightforward to see that dk-aCPA+ implies dk-aCPAn (cf. Def. 22) when $\hat{\mathbf{m}}_0 = \hat{\mathbf{m}}_1$ and dk-aCPAa (cf. Def. 23) when $\mathbf{m}_0 = \mathbf{m}_1$. However, the reverse implication does not hold, even if sk-dualCPA security holds additionally.

Theorem 9 ($\text{dk-aCPAn} \wedge \text{sk-dualCPA} \not\Rightarrow \text{dk-aCPA+}$). For an AME scheme $\text{AME} = (\Pi, \Sigma)$, dk-aCPAn security and sk-dualCPA security together do not imply dk-aCPA+ security.

¹⁴ Catalano, Giunta, and Migliaro [8] considered so-called fully asymmetric security where an anamorphic encryption of $(\mathbf{m}_0, \hat{\mathbf{m}}_0)$ is indistinguishable from an anamorphic encryption of $(\mathbf{m}_1, \hat{\mathbf{m}}_1)$ to the anamorphic sender. However, their notion is defined in the asymmetric setting, i.e., the double key consists of two parts, the double public key $\mathbf{dpk}$ and double secret key $\mathbf{dsk}$, and the anamorphic sender holds $\mathbf{pk}$ and $\mathbf{dsk}$. Inspired by this, we define dk-aCPA+ security in the *symmetric* setting (cf. Def. 4) which is strictly stronger than dk-aCPAn security here.

dk-aCPAa _{Σ, b} ($\mathcal{A}$):	CHAL($m, \hat{m}_0, \hat{m}_1$)
1 : $(pk, sk, dk) \leftarrow \text{aKGen}(1^\lambda)$	1 : if chal $\vee (\hat{m}_0 \neq \hat{m}_1)$: return $\perp$
2 : chal $\leftarrow$ false	2 : chal $\leftarrow$ true
3 : return $\mathcal{A}^{\text{CHAL}}(pk, dk)$	3 : return aEnc(pk, dk, $m, \hat{m}_b$)

Fig. 20. dk-aCPAa security game for AME scheme $\text{AME} = (\Pi, \Sigma)$.

Proof. Let $\widetilde{\text{PKE}} = (\text{KGen}, \text{Enc}, \text{Dec})$ be an IND-CPA secure PKE scheme, and $\widetilde{\text{SE}} = (\text{KGen}, \text{Enc}, \text{Dec})$ be a PR-CT secure symmetric encryption scheme. We construct an AME scheme $\text{AME} = (\Pi = (\text{KGen}, \text{Enc}, \text{Dec}), \Sigma = (\text{aKGen}, \text{aEnc}, \text{aDec}))$ as follows.

- The key generation algorithms returns $(pk, sk) \leftarrow \widetilde{\text{PKE}}.\text{KGen}(1^\lambda)$.
- The anamorphic key generation algorithm returns (pk, sk, dk) , where $(pk, sk) \leftarrow \widetilde{\text{PKE}}.\text{KGen}(1^\lambda)$, and $dk \leftarrow \widetilde{\text{SE}}.\text{KGen}(1^\lambda)$.
- The encryption algorithm returns $ct = (\widetilde{\text{PKE}}.\text{Enc}(pk, m) || str)$, where str is a string randomly sampled from the ciphertext space of $\widetilde{\text{SE}}$.¹⁵
- The anamorphic encryption algorithm returns $ct = (\widetilde{\text{PKE}}.\text{Enc}(pk, m) || \widetilde{\text{SE}}.\text{Enc}(dk, \hat{m}))$.

It is easy to see that $\text{AME} = (\Pi, \Sigma)$ satisfy both dk-aCPAn security (due to IND-CPA security of $\widetilde{\text{PKE}}$) and sk-dualCPA security (due to ciphertext pseudo-randomness of $\widetilde{\text{SE}}$). However, it does not satisfy dk-aCPA+ security, since given dk , one can easily decrypt the partial ciphertext to obtain $\hat{m}_b$, and hence distinguish the experiments $\text{dk-aCPA}^+_{\Sigma, b}(\mathcal{A})$ for $b \in \{0, 1\}$ with advantage 1. $\square$

Theorem 10 (dk-aCPAa $\wedge$ sk-dualCPA $\nRightarrow$ dk-aCPA+). *For an AME scheme $\text{AME} = (\Pi, \Sigma)$, dk-aCPAa security and sk-dualCPA security together do not imply dk-aCPA+ security.*

Proof. Let $\widetilde{\text{AME}}$ be an AME scheme with sk-dualCPA security and dk-aCPAa security, and $\widetilde{\text{SE}} = (\text{KGen}, \text{Enc}, \text{Dec})$ be a PR-CT-secure symmetric encryption scheme. We construct an AME scheme $\text{AME} = (\Pi = (\text{KGen}, \text{Enc}, \text{Dec}), \Sigma = (\text{aKGen}, \text{aEnc}, \text{aDec}))$ as follows.

- The key generation algorithms returns $(pk, sk) \leftarrow \widetilde{\text{AME}}.\text{KGen}(1^\lambda)$.
- The anamorphic key generation algorithm returns $(pk, sk, dk = (dk_1, dk_2))$, where $(pk, sk, dk_1) \leftarrow \widetilde{\text{AME}}.\text{aKGen}(1^\lambda)$, and $dk_2 \leftarrow \widetilde{\text{SE}}.\text{KGen}(1^\lambda)$.

¹⁵ Note that the ciphertext space of $\widetilde{\text{SE}}$ could be infinite depending on the length of the anamorphic message to be encrypted. Here we basically assume a fixed anamorphic message space, and sample the same length each time.

- The encryption algorithm returns $\text{ct} = (\widetilde{\text{AME}}.\text{Enc}(\text{pk}, \text{m}) || \text{str})$, where str is a string randomly sampled from the ciphertext space of $\widetilde{\text{SE}}$.¹⁶
- The anamorphic encryption algorithm returns $\text{ct} = (\widetilde{\text{AME}}.\text{aEnc}(\text{pk}, \text{dk}_1, \text{m}, \hat{\text{m}}) || \widetilde{\text{SE}}.\text{Enc}(\text{dk}_2, \text{m}))$.

It is easy to see that AME satisfy both dk-aCPAa security (due to dk-aCPAa security of $\widetilde{\text{AME}}$ and independence of $\widetilde{\text{SE}}.\text{Enc}(\text{dk}_2, \text{m})$) and sk-dualCPA security (due to ciphertext pseudorandomness of $\widetilde{\text{SE}}$ and sk-dualCPA security of $\widetilde{\text{AME}}$). However, it does not satisfy dk-aCPA+ security, since given dk , one can easily decrypt the symmetric ciphertext part to obtain the normal message m , and hence distinguish the experiments $\text{dk-aCPA} +_{\Sigma, b}(\mathcal{A})$ for $b \in \{0, 1\}$ with advantage 1. $\square$

$\text{dk-aCPA}(n/a/+)$ and sk-aCPAa are incomparable, which we formalise below.

Theorem 11 ($\text{dk-aCPA}(n/a/+) \not\Leftarrow \text{sk-aCPAa}$). *For an AME scheme $\text{AME} = (\Pi, \Sigma)$, $\text{dk-aCPA}(n/a/+)$ does not imply sk-aCPAa , and vice versa.*

Proof. One direction, $\text{dk-aCPAn} \not\Leftarrow \text{sk-aCPAa}$, can be proved via a counterexample such that $\text{dk} = \perp$, and the anamorphic encryption algorithm $\text{aEnc}(\text{m}, \hat{\text{m}})$ returns $\text{PKE}.\text{Enc}(\text{pk}, (\text{m} || \hat{\text{m}}))$ directly, where PKE is an IND-CPA-secure PKE scheme. It is easy to see that given sk , both m and $\hat{\text{m}}$ can be trivially derived and hence sk-aCPAa does not hold. However, it still satisfies dk-aCPAn security ($\text{aEnc}(\text{pk}, \text{dk} = \perp, \text{m}_0, \hat{\text{m}}) \approx \text{aEnc}(\text{pk}, \text{dk} = \perp, \text{m}_1, \hat{\text{m}})$). This also proves that $\text{dk-aCPA}(a/+) \not\Leftarrow \text{sk-aCPAa}$.

The other direction, $\text{dk-aCPA}(n/a/+) \Leftarrow \text{sk-aCPAa}$, can be proved via a construction where sk is contained in dk . Therefore, with the knowledge of dk one is able to perform both normal and anamorphic decryption. $\square$

Remark 14. Theorem 11 highlights how the secret key sk and the double key dk are incomparable. Such inherent incomparability highlights two distinct aspects of security in an AME scheme: security against the dictator and security against the anamorphic sender. As a result, this reminds us to be cautious when designing (or more precisely, deploying) a “secure” AME scheme.

Now we study more relationships among different security notions against the anamorphic sender. Since sk-dualCPA is the most fundamental security property of an AME scheme, we basically assume sk-dualCPA holds in the following.

Theorem 12 ($\text{dk-CPA-AM} (\wedge \text{sk-dualCPA}) \Leftarrow \text{dk-aCPAa} (\wedge \text{sk-dualCPA})$). *For an sk-dualCPA-secure AME scheme $\text{AME} = (\Pi, \Sigma)$, dk-CPA-AM security does not imply dk-aCPAa security, and vice versa.*

¹⁶ As mentioned above, we basically assume a fixed anamorphic message space, and sample the same length each time.

Proof. One direction, $\text{dk-CPA-AM} \wedge \text{sk-dualCPA} \not\Rightarrow \text{dk-aCPAa}$, is established through a counterexample in the proof of Theorem 9, where an anamorphic ciphertext is in the form of

$$(\text{PKE.Enc}(\text{pk}, \text{m}) \parallel \text{SE.Enc}(\text{dk}, \hat{\text{m}})),$$

and dk allows full access to the anamorphic message but does not compromise the security of m .

The other direction, $\text{dk-CPA-AM} \not\Leftarrow \text{dk-aCPAa} \wedge \text{sk-dualCPA}$, is proved through a counterexample where a normal ciphertext is in the form of $(\text{m} \parallel \text{str})$, and an anamorphic ciphertext is in the form of

$$(\text{m} \parallel \text{SE.Enc}(\text{dk}, \text{PKE.Enc}(\text{pk}, \hat{\text{m}}))).$$

In this case, sk-dualCPA is inherited from the PR-CT security of SE , and dk-aCPAa is guaranteed by the IND-CPA security of PKE . However, dk-CPA-AM is not achieved since the normal message m is exposed in plain within the ciphertext. $\square$

Theorem 13 ($\text{dk-aCPAn} \not\Rightarrow \text{dk-CPA-AM}$). *For an AME scheme $\text{AME} = (\Pi, \Sigma)$, dk-aCPAn security does not imply dk-CPA-AM security.*

Proof. Let $\widetilde{\text{AME}} = (\Pi, \Sigma)$ be a dk-aCPAn -secure AME scheme, and AME be as in $\widetilde{\text{AME}}$ except with $\text{Enc}(\text{pk}, \text{m}) = \text{m}$ and $\text{Dec}(\text{sk}, \text{m}) = \text{m}$. Observe that this scheme is still dk-aCPAn -secure, but trivially not dk-CPA-AM secure (since the challenge message is immediately revealed to the adversary). $\square$

Theorem 14 ($\text{dk-aCPAn} \wedge \text{sk-dualCPA} \Rightarrow \text{IND-CPA}$, and $\text{dk-aCPAn} \not\Leftarrow \text{IND-CPA} \wedge \text{sk-dualCPA}$). *For an AME scheme $\text{AME} = (\Pi, \Sigma)$, dk-aCPAn security and sk-dualCPA security together imply IND-CPA security. However, IND-CPA security, even combined with sk-dualCPA security, does not imply dk-aCPAn security.*

Proof. The proof for $\text{dk-aCPAn} \wedge \text{sk-dualCPA} \Rightarrow \text{IND-CPA}$ is similar to the proof of Theorem 3. For $b \in \{0, 1\}$, we first introduce the hybrid game $\text{Hybrid}_{\Pi, \Sigma, b}(\mathcal{A})$ which is the same as $\text{IND-CPA}_{\Pi, b}(\mathcal{A})$ except that the public key pk is generated by $(\text{pk}, \text{dk}, \text{sk}) \leftarrow \Sigma.\text{aKGen}(1^\lambda)$ instead of $(\text{pk}, \text{sk}) \leftarrow \Pi.\text{KGen}(1^\lambda)$, and the challenge ciphertext is computed by $\text{aEnc}(\text{pk}, \text{dk}, \text{m}_b, \hat{\text{m}})$ instead of $\text{Enc}(\text{pk}, \text{m}_b)$ for some $\hat{\text{m}}$ chosen by the adversary.

For $b \in \{0, 1\}$, $\text{Hybrid}_{\Pi, \Sigma, b}(\mathcal{A})$ and $\text{IND-CPA}_{\Pi, b}(\mathcal{A})$ are indistinguishable to the adversary $\mathcal{A}$. Furthermore, any adversary capable of distinguishing $\text{Hybrid}_{\Pi, \Sigma, 1}(\mathcal{A})$ from $\text{Hybrid}_{\Pi, \Sigma, 0}(\mathcal{A})$ (where only pk is provided) can be directly used to distinguish $\text{dk-CPA-AM}_{\Pi, \Sigma, 1}(\mathcal{A})$ and $\text{dk-CPA-AM}_{\Pi, \Sigma, 0}(\mathcal{A})$ (where both pk and dk are provided).

The proof of the opposite direction $\text{dk-aCPAn} \not\Leftarrow \text{IND-CPA} (\wedge \text{sk-dualCPA})$, is illustrated by a counterexample of an AME scheme $\text{AME} = (\Pi, \Sigma)$ where sk

is a part of $\mathbf{dk}$. Therefore, holding $\mathbf{dk}$ is able to perform both decryption and anamorphic decryption, and hence $\mathbf{dk}\text{-aCPA}$ does not hold at all. However, IND-CPA security and sk-dualCPA security may still hold (e.g., the construction in the proof of Theorem 9). $\square$

Corollary 1. *For an AME scheme $\text{AME} = (\Pi, \Sigma)$, $\mathbf{dk}\text{-aCPA} + \text{security}$ and sk-dualCPA security together imply IND-CPA security. However, IND-CPA security, even combined with sk-dualCPA security, does not imply $\mathbf{dk}\text{-aCPA} + \text{security}$.*

Theorem 15 ($\text{IND-CPA} \wedge \text{sk-dualCPA} \Leftrightarrow \mathbf{dk}\text{-aCPA} \wedge \text{sk-dualCPA}$). *For an sk-dualCPA -secure AME scheme $\text{AME} = (\Pi, \Sigma)$, $\mathbf{dk}\text{-CPA-AM}$ security does not imply $\mathbf{dk}\text{-aCPA}$ security, and vice versa.*

The proof is similar to the proof of Theorem 12 and we omit it here.

C Additional Results in the CCA Setting

In this section we present additional security notions in the CCA setting, extending Section 6. Then, we explore relations between different CCA security notions.

Since CCA security is highly related with robustness (cf. Def. 5), we start by discussing more on it. Note that we robustness in the single-challenge setting, differing from the multiple challenge setting by Banfi et al. [1], where the adversary $\mathcal{A}$ has up to a polynomial bound of times to sample message $\mathbf{m}$, and $\mathcal{A}$ wins the security game as long as in one challenge query $\mathbf{aDec}(\mathbf{sk}, \mathbf{dk}, \mathbf{Enc}(\mathbf{pk}, \mathbf{m})) \neq \perp$. Via standard hybrid argument, it is straightforward that robustness in the single-challenge setting implies the robustness in the multiple challenge setting with a loss factor Q , the number of queries made by $\mathcal{A}$.

Remark 15 (Two (Stronger) Variants of ROB-PT). We could further define two stronger variants of ROB-PT reasonably as follows.

- In the first variant, which we refer to as ROB-PT-R, the adversary is additionally allowed to choose the randomness for $\mathbf{Enc}$. This notion applies in the scenarios where the adversary can influence the randomness used in the encryption process. However, it remains weaker than the ROB-CT notion we define below.
- In the second variant, referred to as $\mathbf{dk}\text{-ROB-PT}$, the adversary is additionally access to the double key $\mathbf{dk}$. This notion applies when the adversary (acting as the anamorphic sender) aims to make the dictator aware of the use of anamorphic channel by promoting the dictator to sending a specific message to the receiver, thereby framing the receiver. However, the anamorphic sender avoids submitting the double key to the dictator directly, as doing so would expose them to potential punishment. Note that this notion appears to be incomparable with the ROB-CT notion defined below.

The original definition of robustness by [1] considered only standard ciphertexts generated via normal encryption process. However, beyond these, there exist numerous “non-standard” ciphertexts, such as those produced through improper randomness or entirely adversarial ciphertexts crafted by attackers. To address this, we extend the robustness notion to allow the adversary to select ciphertexts itself and formalize the enhanced notion as ROB-CT, defined below.

Definition 24 (ROB-CT Security of AME). *An AME scheme $\text{AME} = (\Pi, \Sigma)$ is ROB-CT-secure, if, for every PPT adversary $\mathcal{A}$, the advantage*

$$\text{Adv}_{\Pi, \Sigma}^{\text{rob-ct}}(\mathcal{A}) := \Pr[\text{ROB-CT}_{\Pi, \Sigma}(\mathcal{A}) = 1]$$

is negligible in λ , where the experiment $\text{ROB-CT}_{\Pi, \Sigma}(\mathcal{A})$ is defined in Fig. 21.

ROB-CT_{Π,Σ}($\mathcal{A}$): 1 : $(\text{pk}, \text{sk}, \text{dk}) \leftarrow \text{aKGen}(1^\lambda)$ 2 : $\text{ct} \leftarrow \mathcal{A}(\text{pk}, \text{sk})$ 3 : if $\text{aDec}(\text{sk}, \text{dk}, \text{ct}) \neq \perp$: return 1 4 : return 0
--

Fig. 21. ROB-CT security game for AME scheme $\text{AME} = (\Pi, \Sigma)$.

Remark 16. Similar as above, we can define dk-ROB-CT where the adversary additionally obtains the double key dk . We emphasize that this notion does not make sense, since the adversary can always invoke aEnc to result in an anamorphic ciphertext.

Theorem 16 (ROB-CT+ $\Rightarrow$ ROB-CT $\Rightarrow$ ROB-PT, and ROB-CT+ $\not\Leftarrow$ ROB-CT $\not\Leftarrow$ ROB-PT). *For an AME scheme $\text{AME} = (\Pi, \Sigma)$, ROB-CT+ implies ROB-CT, which in turn implies ROB-PT. Conversely, the implications in the opposite direction do not hold.*

Proof. As the forward implications are straightforward to see, we focus on the proof of the opposite direction.

The claim $\text{ROB-CT+} \not\Leftarrow \text{ROB-CT}$ is proved via the following counterexample. Let AE be an authenticated encryption scheme, and PKE be a standard (IND-CPA-secure) PKE scheme. Now we construct an AME scheme whose anamorphic encryption on $(\text{m}, \hat{\text{m}})$ returns

$$\text{ct} = (\text{PKE.Enc}(\text{pk}, \text{m}) || \text{AE.Enc}(\text{dk}, \hat{\text{m}})).$$

ROB-CT of the scheme is guaranteed by the security of AE . However, it does not satisfy ROB-CT+, since given a ciphertext $\text{ct} \leftarrow \text{aEnc}(\text{pk}, \text{dk}, \text{m}, \hat{\text{m}})$, one can

easily replace the first part of ct to another encryption of m and hence obtain a valid anamorphic ciphertext.

Another concrete example occurs in the stateful AME scheme in [1] where in the anamorphic encryption, the randomness r used in encryption is replaced with $r := F_{\text{dk}}(\text{ctr}) \oplus \hat{\text{m}}$. Here $F_{\text{dk}}(\cdot)$ is a secure pseudorandom function (PRF) with key dk , and ctr is a counter kept in state. The scheme satisfies ROB-CT, but not ROB-CT+ due to the malleability of r .

The claim $\text{ROB-CT} \not\Rightarrow \text{ROB-PT}$ is proven by the counterexample of the Koppula-Waters (KW) encryption scheme [18] shown in [25]. In the anamorphic KW encryption, the double key dk (the receiver double key in [25]) is not involved in the anamorphic encryption algorithm. That is, the sender, holding only the public key, can select whether encrypt a message via normal encryption, or encrypt a message as well as an anamorphic message via anamorphic encryption. ROB-PT holds as long as the anamorphic message $\hat{\text{m}} \neq 0^\lambda$ (λ is some global default parameter), which is easily achieved if we just exclude 0^λ from the space of anamorphic messages. However, ROB-CT does not hold at all, since it is easy to generate an anamorphic ciphertext via anamorphic encryption. $\square$

Now we extend sk-aCPAa into sk-aCCAa , and illustrate its relationship with other notions.

Definition 25 (sk-aCCAa Security of AME). *An AME scheme $\text{AME} = (\Pi, \Sigma)$ is sk-aCCAa-secure, if, for every PPT adversary $\mathcal{A}$, the advantage*

$$\text{Adv}_{\Pi, \Sigma}^{\text{sk-accAa}}(\mathcal{A}) := |\Pr[\text{sk-aCCAa}_{\Pi, \Sigma, 1}(\mathcal{A}) = 1] - \Pr[\text{sk-aCCAa}_{\Pi, \Sigma, 0}(\mathcal{A}) = 1]|$$

is negligible in λ , where the experiment $\text{sk-aCCAa}_{\Pi, \Sigma, b}(\mathcal{A})$ for $b \in \{0, 1\}$ is defined in Fig. 22.

$\text{sk-aCCAa}_{\Pi, \Sigma, b}(\mathcal{A})$:	$\text{CHAL}(\text{m}, \hat{\text{m}}_0, \hat{\text{m}}_1)$
1 : $(\text{pk}, \text{sk}, \text{dk}) \leftarrow \text{aKGen}(1^\lambda)$	1 : if $(\text{ct}^* \neq \perp) \vee (\hat{\text{m}}_0 \neq \hat{\text{m}}_1)$: return $\perp$
2 : $\text{ct}^* \leftarrow \perp$	2 : $\text{ct}^* \leftarrow \text{aEnc}(\text{pk}, \text{dk}, \text{m}, \hat{\text{m}}_b)$
3 : return $\mathcal{A}^{\text{AENC}, \text{CHAL}, \text{ADEC}}(\text{pk}, \text{sk})$	3 : return ct^*
$\text{AENC}(\text{m}, \hat{\text{m}})$	$\text{ADEC}(\text{ct})$
1 : return $\text{aEnc}(\text{pk}, \text{dk}, \text{m}, \hat{\text{m}})$	1 : if $\text{ct} = \text{ct}^*$: return $\perp$
	2 : return $\text{aDec}(\text{sk}, \text{dk}, \text{ct})$

Fig. 22. sk-aCCAa security game for AME scheme $\text{AME} = (\Pi, \Sigma)$.

Theorem 17 (sk-dualCCA $\Rightarrow$ sk-aCCAa). *For an AME scheme $\text{AME} = (\Pi, \Sigma)$, sk-dualCCA security implies sk-aCCAa security.*

Proof. The proof is similar to the proof of Theorem 8. To argue that $\text{sk-aCCAA}_{\Pi,\Sigma,1}(\mathcal{A})$ is indistinguishable from $\text{sk-aCCAA}_{\Pi,\Sigma,0}(\mathcal{A})$, we introduce a hybrid game $\text{Hybrid}_{\Pi,\Sigma,b}(\mathcal{A})$ for $b \in \{0,1\}$, which is exactly the experiment $\text{sk-aCCAA}_{\Sigma,b}(\mathcal{A})$ except that $(\text{pk}, \text{sk}, \text{dk}) \leftarrow \text{aKGen}(1^\lambda)$ is replaced with $(\text{pk}, \text{sk}) \leftarrow \text{KGen}(1^\lambda)$, $\text{aEnc}(\text{pk}, \text{dk}, \text{m}, \hat{\text{m}}_b)$ in the encryption challenge oracle is replaced with $\text{Enc}(\text{pk}, \text{m})$, and all decryption queries are replied with $\perp$.

According to the sk-dualCCA security, for $b \in \{0,1\}$, the hybrid experiment $\text{Hybrid}_{\Pi,\Sigma,b}(\mathcal{A})$ and $\text{sk-aCCAA}_{\Pi,\Sigma,b}(\mathcal{A})$ are indistinguishable to the adversary $\mathcal{A}$. Consequently, $\text{Hybrid}_{\Pi,\Sigma,1}(\mathcal{A})$ and $\text{Hybrid}_{\Pi,\Sigma,0}(\mathcal{A})$ are identical since the challenge ciphertext is independent of $\hat{\text{m}}_b$, which finishes the proof. $\square$

Theorem 18 (sk-aCCAA $\not\Rightarrow$ ROB-CT+). *For an AME scheme $\text{AME} = (\Pi, \Sigma)$, sk-aCCAA does not imply ROB-CT+ and vice versa.*

Proof. We first prove $\text{sk-aCCAA} \not\Rightarrow \text{ROB-CT+}$. The high-level idea is to let the public key contains a valid message-ciphertext pair for anamorphic encryption, hence failing the ROB-CT+ property. Let SE be an IND-CCA secure symmetric encryption scheme with dk the symmetric key (recall that sk-aCCAA requires only the security of anamorphic encryption, but not normal encryption). We construct an AME scheme with anamorphic triplet Σ as follows.

- The anamorphic key generation returns $(\text{pk}, \text{sk}, \text{dk})$, where $\text{dk} \leftarrow \text{SE.KGen}(1^\lambda)$, $\text{sk} := \perp$, and $\text{pk} := ((\text{m}_\pi, \hat{\text{m}}_\pi), \text{ct}_\pi)$ is a message-ciphertext pair with some random messages $(\text{m}_\pi, \hat{\text{m}}_\pi)$ and $\text{ct}_\pi := (\tilde{\text{ct}}, \text{m}_\pi)$ with $\tilde{\text{ct}} \leftarrow \text{SE.Enc}(\text{dk}, (\text{m}_\pi, \hat{\text{m}}_\pi))$.
- The anamorphic encryption algorithm $\text{aEnc}(\text{pk}, \text{dk}, \text{m}, \hat{\text{m}})$ returns $\text{ct} := (\text{SE.Enc}(\text{dk}, (\text{m}, \hat{\text{m}})), \text{m})$. Note that the normal message m is exposed in plain, but it does not affect the sk-aCCAA security, which focuses only on the security of anamorphic encryption (and the basic correctness).
- The decryption algorithm $\tilde{\text{Enc}}(\text{sk}, \text{ct} = (\tilde{\text{ct}}, \text{m}))$ returns m directly.
- The anamorphic decryption algorithm $\text{aDec}(\text{sk}, \text{dk}, \text{ct} = (\tilde{\text{ct}}, \text{m}))$ first takes the symmetric decryption to obtain $(\text{m}', \hat{\text{m}}) \leftarrow \text{SE.Dec}(\text{dk}, \tilde{\text{ct}})$ (this step might returns $\perp$ due to the CCA property of SE), and returns $\hat{\text{m}}$ if $\text{m}' = \text{m}$ and $\perp$ otherwise.

It is straightforward to see that if SE has IND-CCA security, then Σ satisfies both correctness and sk-aCCAA security. However, given pk which contains a message-ciphertext pair from anamorphic encryption, one can easily breaks the ROB-CT+ security by just outputting ct_π .

Now we prove $\text{sk-aCCAA} \not\Leftarrow \text{ROB-CT+}$. This direction is obvious since ROB-CT+ requires nothing about the confidentiality of either m or $\hat{\text{m}}$. Therefore, any signature scheme with strong unforgeability can be transferred into an anamorphic triplet with ROB-CT+ security, where dk is the signing secret key, $\text{aEnc}(\text{pk}, \text{dk}, \text{m}, \hat{\text{m}})$ returns $\text{ct} := (\text{m}, \hat{\text{m}}, \sigma)$ with σ a signature of $(\text{m}, \hat{\text{m}})$, and $\text{aDec}(\text{sk}, \text{dk}, \text{ct})$ returns $\hat{\text{m}}$ if σ is a valid signature. ROB-CT+ is inherited from the strong unforgeability of the signature scheme. However, it is obvious that

this scheme does not have sk-aCCAA security at all. (Even more, it is not a CPA secure encryption scheme!) $\square$

Similar to the CPA setting, we define dk-aCCA(n/a) to present the security of the normal message or the anamorphic message in an anamorphic ciphertext.

Definition 26 (dk-aCCAn Security of AME). An AME scheme $\text{AME} = (\Pi, \Sigma)$ is dk-aCCAn-secure, if, for every PPT adversary $\mathcal{A}$, the advantage

$$\text{Adv}_{\Pi, \Sigma}^{\text{dk-accan}}(\mathcal{A}) := |\Pr[\text{dk-aCCAn}_{\Pi, \Sigma, 1}(\mathcal{A}) = 1] - \Pr[\text{dk-aCCAn}_{\Pi, \Sigma, 0}(\mathcal{A}) = 1]|$$

is negligible in λ , where the experiment $\text{dk-aCCAn}_{\Pi, \Sigma, b}(\mathcal{A})$ for $b \in \{0, 1\}$ is defined in Fig. 23.

$\text{dk-aCCAn}_{\Pi, \Sigma, b}(\mathcal{A})$:	$\text{CHAL}(\mathbf{m}_0, \mathbf{m}_1, \hat{\mathbf{m}})$
1 : $(\text{pk}, \text{sk}, \text{dk}) \leftarrow \text{aKGen}(1^\lambda)$	1 : if $(\text{ct}^* \neq \perp) \vee (\mathbf{m}_0 \neq \mathbf{m}_1)$: return $\perp$
2 : $\text{ct}^* \leftarrow \perp$	2 : $\text{ct}^* \leftarrow \text{aEnc}(\text{pk}, \text{dk}, \mathbf{m}_b, \hat{\mathbf{m}})$
3 : return $\mathcal{A}^{\text{CHAL}, \text{DEC}, \text{ADEC}}(\text{pk}, \text{dk})$	3 : return ct^*
$\text{DEC}(\text{ct})$	$\text{ADEC}(\text{ct})$
1 : if $\text{ct} = \text{ct}^*$: return $\perp$	1 : return $\text{aDec}(\text{sk}, \text{dk}, \text{ct})$
2 : return $\text{Dec}(\text{sk}, \text{ct})$	

Fig. 23. dk-aCCAn security game for AME scheme $\text{AME} = (\Pi, \Sigma)$.

Definition 27 (dk-aCCAA Security of AME). An AME scheme $\text{AME} = (\Pi, \Sigma)$ is dk-aCCAA-secure, if, for every PPT adversary $\mathcal{A}$, the advantage

$$\text{Adv}_{\Pi, \Sigma}^{\text{dk-accaa}}(\mathcal{A}) := |\Pr[\text{dk-aCCAA}_{\Pi, \Sigma, 1}(\mathcal{A}) = 1] - \Pr[\text{dk-aCCAA}_{\Pi, \Sigma, 0}(\mathcal{A}) = 1]|$$

is negligible in λ , where the experiment $\text{dk-aCCAA}_{\Pi, \Sigma, b}(\mathcal{A})$ for $b \in \{0, 1\}$ is defined in Fig. 24.

As in the CPA setting, dk-aCCA+ implies dk-aCCAn when $\hat{\mathbf{m}}_0 = \hat{\mathbf{m}}_1$, and dk-aCCAA when $\mathbf{m}_0 = \mathbf{m}_1$. The proof is straightforward, but we still emphasize that the anamorphic decryption in dk-aCCA+ (which is not allowed to query the challenge ciphertext) is more strict than that in dk-aCCAn, and the decryption oracle (which is not allowed to query the challenge ciphertext) is more strict than that in dk-aCCAA.

However, this is not an issue in the proof. Take the reduction from dk-aCCAn to dk-aCCA+ as an example. In the reduction from switching a dk-aCCAn adversary $\mathcal{A}$ (where $\mathcal{A}$ samples $\mathbf{m}_0, \mathbf{m}_1, \hat{\mathbf{m}}$ to the challenge oracle) to a dk-aCCA+ adversary $\mathcal{A}'$ (where $\mathcal{A}'$ samples $\mathbf{m}_0, \mathbf{m}_1, \hat{\mathbf{m}}_0, \hat{\mathbf{m}}_1$ to the challenge oracle), $\mathcal{A}'$ will

dk-aCCA _{aΠ, Σ, b} ($\mathcal{A}$):	CHAL($m, \hat{m}_0, \hat{m}_1$)
1 : $(pk, sk, dk) \leftarrow \text{aKGen}(1^\lambda)$	1 : if $(ct^* \neq \perp) \vee (\hat{m}_0 \neq \hat{m}_1)$: return $\perp$
2 : $ct^* \leftarrow \perp$	2 : $ct^* \leftarrow \text{aEnc}(pk, dk, m, \hat{m}_b)$
3 : return $\mathcal{A}^{\text{CHAL}, \text{DEC}, \text{ADEC}}(pk, dk)$	3 : return ct^*
DEC(ct)	ADEC(ct)
1 : return Dec(sk, ct)	1 : if $ct = ct^*$: return $\perp$
	2 : return aDec(sk, dk, ct)

Fig. 24. dk-aCCAa security game for AME scheme $\text{AME} = (\Pi, \Sigma)$.

sets $\hat{m}_0 = \hat{m}_1 = \hat{m}$ and passes the challenge ciphertext obtained from its challenger to $\mathcal{A}$. Later whenever $\mathcal{A}$ asks an anamorphic decryption query of the challenge ciphertext ct^* (since this query is allowed in the dk-aCCAn experiment), $\mathcal{A}'$ directly returns $\hat{m}$. Due to the correctness of AME, this is statistically close to the experiment where the result $\text{aDec}(sk, dk, ct^*)$ is returned. The argument for the reduction from dk-aCCAa to dk-aCCA+ is analogous.

Theorem 19 (dk-aCCAn $\wedge$ sk-dualCCA $\nRightarrow$ dk-aCCA+). *For an AME scheme $\text{AME} = (\Pi, \Sigma)$, dk-aCCAn security and sk-dualCCA security together do not imply dk-aCCA+ security.*

Proof. Let $\widetilde{\text{AME}}$ be an AME scheme satisfying dk-aCCAn and sk-dualCCA (e.g., the randomness-recoverable CCA PKE with randomness = $\text{AE.Enc}(dk_1, \hat{m})$), and $1_{\mathcal{M}}$ be an anamorphic message belongs to the anamorphic message space of $\widetilde{\text{AME}}$. We construct another AME scheme with anamorphic message space $\{0, 1\}$ satisfying the first two properties but not dk-aCCA+ as follows.

- The anamorphic key generation algorithm returns $pk, sk, dk = (dk_1, dk_2)$, where $(pk, sk, dk_1) \leftarrow \widetilde{\text{AME.aKGen}}(1^\lambda)$, and dk_2 is a randomly sampled key of a pseudorandom function (PRF) F .
- The encryption algorithm $\text{Enc}(pk, m)$ returns $ct = \widetilde{\text{AME.Enc}}(pk, m)$.
- The anamorphic encryption algorithm $\text{aEnc}(pk, dk, m, \hat{m})$ returns $ct = \widetilde{\text{AME.aEnc}}(pk, dk_1, m, 1_{\mathcal{M}})$ such that $F_{dk_2}(ct) = \hat{m}$ (note that $\hat{m} \in \{0, 1\}$).
- The anamorphic decryption algorithm aDec returns $F_{dk_2}(ct)$ if $\widetilde{\text{AME.aDec}}(sk, dk_1, ct) = 1_{\mathcal{M}}$, and $\perp$ otherwise.

The construction above inherits dk-aCCAn and sk-dualCCA from $\widetilde{\text{AME}}$. However, it does not satisfy dk-aCCA+, since given $dk = (dk_1, dk_2)$ and an anamorphic ciphertext $ct = \text{aEnc}(pk, dk, m, \hat{m})$, one can easily outputs the anamorphic ciphertext $F_{dk_2}(ct)$ (by correctness it must hold that $\widetilde{\text{AME.aDec}}(sk, dk_1, ct) = 1_{\mathcal{M}}$). $\square$

Theorem 20 ($\mathbf{dk-aCCAa} \wedge \mathbf{sk-dualCCA} \not\Rightarrow \mathbf{dk-aCCA+}$). *For an AME scheme $\text{AME} = (\Pi, \Sigma)$, $\mathbf{dk-aCCAa}$ security and $\mathbf{sk-dualCCA}$ security together do not imply $\mathbf{dk-aCCA+}$ security.*

The proof is similar to the proof above, except that the anamorphic encryption algorithm returns $\text{ct} = \widetilde{\text{AME}}.\text{aEnc}(\text{pk}, \text{dk}_1, \text{m}, \hat{\text{m}})$ such that $F_{\text{dk}_2}(\text{ct}) = \text{m}$ (similarly we assume the normal message space is $\{0, 1\}$). We omit the details here.

Similar to the CPA setting, we argue that $\mathbf{dk-aCCA(n/a/+)}$ and $\mathbf{sk-aCCAa}$ are incomparable via the following theorem.

Theorem 21 ($\mathbf{dk-aCCA(n/a/+)} \not\Rightarrow \mathbf{sk-aCCAa}$). *For an AME scheme $\text{AME} = (\Pi, \Sigma)$, $\mathbf{dk-aCCA(n/a/+)}$ does not imply $\mathbf{sk-aCCAa}$, and vice versa.*

The proof is similar to the proof of Theorem 11 and we omit it here.

Theorem 22 ($\mathbf{dk-CCA-AM} \wedge \mathbf{sk-dualCCA} \not\Rightarrow \mathbf{dk-aCCAa} \wedge \mathbf{sk-dualCCA}$). *For an $\mathbf{sk-dualCCA}$ -secure AME scheme $\text{AME} = (\Pi, \Sigma)$, $\mathbf{dk-CCA-AM}$ security does not imply $\mathbf{dk-aCCAa}$ security, and vice versa.*

Proof. We first prove that $\mathbf{dk-CCA-AM} \wedge \mathbf{sk-dualCCA} \not\Rightarrow \mathbf{dk-aCCAa}$. Let $\widetilde{\text{AME}}$ be an AME scheme satisfying $\mathbf{dk-CCA-AM}$ and $\mathbf{sk-dualCCA}$ (cf. the examples in the next section), and $1_{\mathcal{M}}$ be an anamorphic message belongs to the anamorphic message space of $\widetilde{\text{AME}}$. Similar to the proof of Theorem 19, we construct another AME scheme with anamorphic message space $\{0, 1\}$ satisfying the first two properties but not $\mathbf{dk-aCCAa}$ as follows.

- The key generation algorithm returns $(\text{pk}, \text{sk}) \leftarrow \widetilde{\text{AME}}.\text{KGen}(1^\lambda)$.
- The anamorphic key generation algorithm returns $\text{pk}, \text{sk}, \text{dk} = (\text{dk}_1, \text{dk}_2)$, where $(\text{pk}, \text{sk}, \text{dk}_1) \leftarrow \widetilde{\text{AME}}.\text{aKGen}(1^\lambda)$, and dk_2 is a randomly sampled key of a pseudorandom function F .
- The encryption algorithm $\text{Enc}(\text{pk}, \text{m})$ returns $\text{ct} = \widetilde{\text{AME}}.\text{Enc}(\text{pk}, \text{m})$.
- The anamorphic encryption algorithm $\text{aEnc}(\text{pk}, \text{dk}, \text{m}, \hat{\text{m}})$ returns $\text{ct} = \widetilde{\text{AME}}.\text{aEnc}(\text{pk}, \text{dk}_1, \text{m}, 1_{\mathcal{M}})$ such that $F_{\text{dk}_2}(\text{ct}) = \hat{\text{m}}$ (note that $\hat{\text{m}} \in \{0, 1\}$).
- The decryption algorithm $\text{Dec}(\text{sk}, \text{ct})$ returns $\widetilde{\text{AME}}.\text{Dec}(\text{sk}, \text{ct})$.
- The anamorphic decryption algorithm aDec returns $F_{\text{dk}_2}(\text{ct})$ if $\widetilde{\text{AME}}.\text{aDec}(\text{sk}, \text{dk}_1, \text{ct}) = 1_{\mathcal{M}}$, and $\perp$ otherwise.

The construction above inherits $\mathbf{dk-CCA-AM}$ and $\mathbf{sk-dualCCA}$ from $\widetilde{\text{AME}}$. However, it does not satisfy $\mathbf{dk-aCCAa}$, since given $\text{dk} = (\text{dk}_1, \text{dk}_2)$ and an anamorphic ciphertext $\text{ct} = \text{aEnc}(\text{pk}, \text{dk}, \text{m}, \hat{\text{m}})$, one can easily outputs the anamorphic ciphertext $F_{\text{dk}_2}(\text{ct})$ (by correctness it must hold that $\widetilde{\text{AME}}.\text{aDec}(\text{sk}, \text{dk}_1, \text{ct}) = 1_{\mathcal{M}}$).

The other direction, to prove $\mathbf{dk-CCA-AM} \not\Rightarrow \mathbf{dk-aCCAa} \wedge \mathbf{sk-dualCCA}$, we construct an AME scheme where the normal message is exposed in plain in the ciphertexts (note, however, that it should still ensure the CCA security of the anamorphic message). More precisely, assume $\widetilde{\text{AME}}$ is an AME scheme satisfying $\mathbf{dk-aCCAa}$ and $\mathbf{sk-dualCCA}$, we construct AME as follows.

- The key generation algorithm returns $(pk, sk) \leftarrow \widehat{AME}.KGen(1^\lambda)$.
- The anamorphic key generation algorithm returns $(pk, sk, dk) \leftarrow \widehat{AME}.aKGen(1^\lambda)$.
- The encryption algorithm $Enc(pk, m)$ returns $ct = (m, \hat{ct})$, where $\hat{ct} \leftarrow \widehat{AME}.Enc(pk, m)$.
- The anamorphic encryption algorithm $aEnc(pk, dk, m, \hat{m})$ returns $ct := (m || \hat{ct})$, where $\hat{ct} \leftarrow \widehat{AME}.aEnc(pk, dk, m, \hat{m})$.
- The decryption algorithm $Dec(sk, ct = (m || \hat{ct}))$ returns m if $\widehat{AME}.Dec(sk, \hat{ct}) = m$, and $\perp$ otherwise.
- The anamorphic decryption algorithm $aDec(sk, dk, ct = (m || \hat{ct}))$ returns $\widehat{AME}.aDec(sk, dk, \hat{ct})$ if $\widehat{AME}.Dec(sk, \hat{ct}) = m$, and $\perp$ otherwise.¹⁷

dk-aCCAA and sk-dualCCA of AME are inherited from $\widehat{AME}$. However, AME does not satisfy dk-CCA-AM at all, since the message is exposed in plain in the ciphertexts. $\square$

Now we investigate the relationships among different security notions against the anamorphic sender. Since sk-dualCCA is the most fundamental security property of an AME scheme in the CCA setting, in the following we basically assume sk-dualCCA holds.

Relations between dk-CCA-AM and dk-aCCA(n/+). Similar to the CPA setting, we prove the following theorem.

Theorem 23 (dk-CCA-AM $(\wedge$ sk-dualCCA) $\not\Rightarrow$ dk-aCCA(n/+)). *For an AME scheme $AME = (\Pi, \Sigma)$, dk-CCA-AM security and sk-dualCCA security together do not imply either dk-aCCAn security, or dk-aCCA+ security.*

Proof. Since dk-aCCA+ is strictly stronger than dk-aCCAn, it is sufficient to prove that dk-CCA-AM $(\wedge$ sk-dualCCA) $\not\Rightarrow$ dk-aCCAn. Let $\widetilde{AME}$ be a dk-CCA-AM-secure and sk-dualCCA secure AME scheme. We construct an AME scheme AME with normal message space $\{0, 1\}$ as follows.

- The key generation algorithm returns $(pk, sk) \leftarrow \widetilde{AME}.KGen(1^\lambda)$.
- The anamorphic key generation algorithm returns $pk, sk, dk = (dk_1, dk_2)$, where $(pk, sk, dk_1) \leftarrow \widetilde{AME}.aKGen(1^\lambda)$, and dk_2 is a randomly sampled key of a pseudorandom function F .
- The encryption algorithm $Enc(pk, m)$ returns $ct = \widetilde{AME}.Enc(pk, m)$.
- The anamorphic encryption algorithm $aEnc(pk, dk, m, \hat{m})$ returns $ct = \widetilde{AME}.aEnc(pk, dk_1, m, \hat{m})$ such that $F_{dk_2}(ct) = m$ (note that $m \in \{0, 1\}$).
- The decryption algorithm $Dec(sk, ct)$ returns $\widetilde{AME}.Dec(sk, ct)$.
- The anamorphic decryption algorithm $aDec$ returns $\widetilde{AME}.aDec(sk, dk_1, ct)$.

¹⁷ We emphasize that it is vital to ensure the normal encryption would not return $\perp$ before returning the anamorphic decryption result, as otherwise CCA security would not hold.

dk-CCA-AM security and sk-dualCCA security are inherited from $\widetilde{\text{AME}}$. However, it is easy to see that the compromise of dk_2 will totally break the confidentiality of m in the anamorphic ciphertext generated via aEnc . Namely, AME does not satisfy dk-aCCAn at all, concluding the proof. $\square$

However, similar to the CPA setting, it is unknown whether the implication from dk-aCCA(n/+) and sk-dualCCA to dk-CCA-AM holds or not.

Theorem 24 (dk-CCA-AM $\wedge$ sk-dualCCA $\Rightarrow$ IND-CCA, and dk-CCA-AM $\not\Leftarrow$ IND-CCA ($\wedge$ sk-dualCCA)). *For an AME scheme $\text{AME} = (\Pi, \Sigma)$, dk-CCA-AM security and sk-dualCCA security together imply IND-CCA security. However, IND-CCA security, even combined with sk-dualCCA security, does not imply dk-CCA-AM security.*

Proof. We first prove $\text{dk-CCA-AM} \wedge \text{sk-dualCCA} \Rightarrow \text{IND-CCA}$. Consider an AME scheme (Π, Σ) . We prove this theorem by showing that conditioned on sk-dualCCA, an adversary that breaks IND-CCA security can be transformed into another adversary that breaks dk-CCA-AM security.

For $b \in \{0, 1\}$, define the hybrid game $\text{Hybrid}_{\Pi, \Sigma, b}(\mathcal{A})$ which is the same as the $\text{IND-CCA}_{\Pi, b}(\mathcal{A})$ except that the public key pk is generated by $(\text{pk}, \text{sk}, \text{dk}) \leftarrow \Sigma.\text{aKGen}(1^\lambda)$ instead of $(\text{pk}, \text{sk}) \leftarrow \Pi.\text{KGen}(1^\lambda)$.

Thanks to sk-dualCCA security, $\text{Hybrid}_{\Pi, \Sigma, b}(\mathcal{A})$ and $\text{IND-CCA}_{\Pi, b}(\mathcal{A})$ are indistinguishable to the adversary $\mathcal{A}$ (similar to Lemma 1 but in the CCA setting). Furthermore, any adversary $\mathcal{A}$ capable of distinguishing $\text{Hybrid}_{\Pi, \Sigma, 1}(\mathcal{A})$ from $\text{Hybrid}_{\Pi, \Sigma, 0}(\mathcal{A})$ (where only pk is provided) can be directly used to distinguish $\text{dk-CCA-AM}_{\Pi, \Sigma, 1}(\mathcal{A})$ and $\text{dk-CCA-AM}_{\Pi, \Sigma, 0}(\mathcal{A})$ (where both pk and dk are provided).

The proof of the opposite direction is straightforward since both IND-CCA security and sk-dualCCA security assume that the adversary gets no information with the double key dk . If sk is contained in dk then the normal message m is revealed immediately, and hence dk-CCA-AM does not hold. $\square$

Theorem 25 (dk-aCCAn $\wedge$ sk-dualCCA $\Rightarrow$ IND-CCA, and dk-aCCAn $\not\Leftarrow$ IND-CCA ($\wedge$ sk-dualCCA)). *For an AME scheme $\text{AME} = (\Pi, \Sigma)$, dk-aCCA security and sk-dualCCA security together imply the IND-CCA security. However, IND-CCA security, even combined with sk-dualCCA security, does not imply dk-aCCAn security.*

Proof. We first prove $\text{dk-aCCAn} \wedge \text{sk-dualCCA} \Rightarrow \text{IND-CCA}$. For $b \in \{0, 1\}$, we introduce the hybrid game $\text{Hybrid}_{\Pi, \Sigma, b}(\mathcal{A})$ which is the same as $\text{IND-CCA}_{\Pi, b}(\mathcal{A})$ except that the public key pk is generated by $(\text{pk}, \text{dk}, \text{sk}) \leftarrow \text{aKGen}(1^\lambda)$ instead of $(\text{pk}, \text{sk}) \leftarrow \text{KGen}(1^\lambda)$, and the challenge ciphertext is computed by $\text{aEnc}(\text{pk}, \text{dk}, m_b, \hat{m})$ instead of $\text{Enc}(\text{pk}, m_b)$ for some $\hat{m}$ chosen by the adversary.

For $b \in \{0, 1\}$, $\text{Hybrid}_{\Pi, \Sigma, b}(\mathcal{A})$ and $\text{IND-CCA}_{\Pi, b}(\mathcal{A})$ are indistinguishable to the adversary $\mathcal{A}$ due to the sk-dualCCA security. More precisely, we can construct a reduction algorithm $\mathcal{A}'$ that breaks sk-dualCCA as long as $\mathcal{A}$ can distinguish $\text{Hybrid}_{\Pi, \Sigma, b}(\mathcal{A})$ from $\text{IND-CCA}_{\Pi, b}(\mathcal{A})$. $\mathcal{A}'$ simulates either $\text{Hybrid}_{\Pi, \Sigma, b}(\mathcal{A})$ or $\text{IND-CCA}_{\Pi, b}(\mathcal{A})$ for $\mathcal{A}$ as follows:

- $\mathcal{A}'$ receives $(\mathbf{pk}, \mathbf{sk})$ from its sk-dualCCA security experiment challenger, and passes $\mathbf{pk}$ to $\mathcal{A}$. Here $(\mathbf{pk}, \mathbf{sk}) \leftarrow \text{KGen}(1^\lambda)$ if $\mathcal{A}'$ is accessing the experiment $\text{sk-dualCCA}_{\Pi, \Sigma, 0}(\mathcal{A}')$ (the normal mode), and $(\mathbf{pk}, \mathbf{sk}, \mathbf{dk}) \leftarrow \text{aKGen}(1^\lambda)$ if $\mathcal{A}'$ is accessing the experiment $\text{sk-dualCCA}_{\Pi, \Sigma, 1}(\mathcal{A}')$ (the anamorphic mode).
- Whenever $\mathcal{A}$ asks the challenge oracle with $(\mathbf{m}_0, \mathbf{m}_1)$, $\mathcal{A}'$ randomly samples $\hat{\mathbf{m}}$, sends $(\mathbf{m}_b, \hat{\mathbf{m}})$ to its challenger, and passes the received $\mathbf{ct}^*$ to $\mathcal{A}$ directly.
- Whenever $\mathcal{A}$ asks a decryption query with $\mathbf{ct} \neq \mathbf{ct}^*$, the reduction algorithm $\mathcal{A}'$ returns $\text{Dec}(\mathbf{sk}, \mathbf{ct})$ (recall that $\mathcal{A}'$ holds $\mathbf{sk}$).
- Finally $\mathcal{A}'$ outputs what $\mathcal{A}$ outputs.

For $b \in \{0, 1\}$, if $\mathcal{A}'$ is accessing the experiment $\text{sk-dualCCA}_{\Pi, \Sigma, 0}(\mathcal{A}')$ (the normal mode), then $\mathcal{A}'$ simulates $\text{IND-CCA}_{\Pi, b}(\mathcal{A})$ for $\mathcal{A}$, and if $\mathcal{A}'$ is accessing the experiment $\text{sk-dualCCA}_{\Pi, \Sigma, 1}(\mathcal{A}')$ (the anamorphic mode), then $\mathcal{A}'$ simulates $\text{Hybrid}_{\Pi, \Sigma, b}(\mathcal{A})$ for $\mathcal{A}$. Therefore, $\text{Hybrid}_{\Pi, \Sigma, b}(\mathcal{A})$ and $\text{IND-CCA}_{\Pi, b}(\mathcal{A})$ are indistinguishable to the adversary $\mathcal{A}$ due to sk-dualCCA security.

Finally, any adversary capable of distinguishing $\text{Hybrid}_{\Pi, \Sigma, 1}(\mathcal{A})$ from $\text{Hybrid}_{\Pi, \Sigma, 0}(\mathcal{A})$ (where only $\mathbf{pk}$ is provided) can be directly used to distinguish $\text{dk-CCA-AM}_{\Pi, \Sigma, 1}(\mathcal{A})$ and $\text{dk-CCA-AM}_{\Pi, \Sigma, 0}(\mathcal{A})$ (where both $\mathbf{pk}$ and $\mathbf{dk}$ are provided).

The proof of $\text{dk-aCCAn} \not\Leftarrow \text{IND-CCA} (\wedge \text{sk-dualCCA})$, is implied by an AME scheme where $\mathbf{sk}$ is a part of $\mathbf{dk}$. Therefore, holding $\mathbf{dk}$ is able to do both the normal decryption and the anamorphic decryption, and hence dk-aCCAn does not hold at all. However, IND-CCA security and sk-dualCCA security may still hold. $\square$

Corollary 2. *For an AME scheme $\text{AME} = (\Pi, \Sigma)$, $\text{dk-aCCA} + \text{security}$ and sk-dualCCA security together imply IND-CCA security. However, IND-CCA security, combined with sk-dualCCA security, does not imply $\text{dk-aCCA} + \text{security}$.*

Finally, we prove that IND-CCA and dk-aCCAa are comparable, even conditioned on sk-dualCCA security. This is straightforward since IND-CCA ensures the confidentiality of the normal message $\mathbf{m}$, while dk-aCCAa ensures the confidentiality of the anamorphic message $\hat{\mathbf{m}}$.

Theorem 26 ($\text{IND-CCA} (\wedge \text{sk-dualCCA}) \not\Leftarrow \text{dk-aCCAa} (\wedge \text{sk-dualCCA})$). *For an sk-dualCCA-secure AME scheme $\text{AME} = (\Pi, \Sigma)$, IND-CCA security does not imply dk-aCCAa security, and vice versa.*

Proof. On one direction that $\text{IND-CCA} \wedge \text{sk-dualCCA} \not\Leftarrow \text{dk-aCCAa}$, we construct a counterexample of AME where $\mathbf{dk}$ provides the full access to $\hat{\mathbf{m}}$ in an anamorphic ciphertext, which is the same as the first example in the proof of Theorem 22

On the other direction that $\text{IND-CCA} \not\Leftarrow \text{dk-aCCAa} \wedge \text{sk-dualCCA}$, we construct a counterexample of AME where the normal message $\mathbf{m}$ is exposed in plain in ciphertexts, which is the same as the second example in the proof of Theorem 22. $\square$

D Additional Results for Asymmetric AME

In this section we supply the results of asymmetric AME, where the double key dk is divided into two parts, the sender double key sdk and the receiver double key rdk .

D.1 Security of AAME against the Dictator

The security of AAME against the dictator makes no much difference with that in the symmetric setting. For the integrality of the whole picture, we put the formal definitions as follows.

Definition 28 (sk-dualCPA/sk-dualCCA Security of Asymmetric AME). *An AAME scheme $\text{AAME} = (\Pi, \Sigma)$ is sk-dualX-secure for $X \in \{\text{CPA}, \text{CCA}\}$, if, for every PPT adversary $\mathcal{A}$, the advantage*

$$\text{Adv}_{\Pi, \Sigma}^{\text{sk-dualX}}(\mathcal{A}) := |\Pr[\text{sk-dualX}_{\Pi, \Sigma, 1}(\mathcal{A}) = 1] - \Pr[\text{sk-dualX}_{\Pi, \Sigma, 0}(\mathcal{A}) = 1]|$$

is negligible in λ , where the experiment $\text{sk-dualX}_{\Pi, \Sigma, b}(\mathcal{A})$ for $b \in \{0, 1\}$ is defined in Fig. 25.

$\text{sk-dualX}_{\Pi, \Sigma, b}(\mathcal{A})$:	$\text{CHAL}(\text{m}, \hat{\text{m}})$
1: if $b = 0$:	1: if $\text{ct}^* \neq \perp$: return
2: $(\text{pk}, \text{sk}) \leftarrow \text{KGen}(1^\lambda)$	2: if $b = 0$:
3: else :	3: $\text{ct}^* \leftarrow \text{Enc}(\text{pk}, \text{m})$
4: $(\text{pk}, \text{sk}, \text{sdk}, \text{rdk}) \leftarrow \text{aKGen}(1^\lambda)$	4: else :
5: $\text{ct}^* \leftarrow \perp$	5: $\text{ct}^* \leftarrow \text{aEnc}(\text{pk}, \text{sdk}, \text{m}, \hat{\text{m}})$
6: return $\mathcal{A}^{\text{CHAL}}(\text{pk}, \text{sk})$	6: return ct^*
7: return $\mathcal{A}^{\text{CHAL}, \text{ADec}}(\text{pk}, \text{sk})$	ADec (ct)
	1: if $b = 0 \vee \text{ct} = \text{ct}^*$: return $\perp$
	2: return $\text{aDec}(\text{sk}, \text{rdk}, \text{ct})$

Fig. 25. sk-dualX security game for asymmetric AME scheme $\text{AAME} = (\Pi, \Sigma)$ for $X \in \{\text{CPA}, \text{CCA}\}$. Boxed code is only relevant in the sk-dualCPA game. Highlighted code is only relevant in the sk-dualCCA game.

Definition 29 (sk-aCPAa/sk-aCCAa Security of Asymmetric AME). *An AAME scheme $\text{AAME} = (\Pi, \Sigma)$ is sk-aXa-secure for $X \in \{\text{CPA}, \text{CCA}\}$, if, for every PPT adversary $\mathcal{A}$, the advantage*

$$\text{Adv}_{\Pi, \Sigma}^{\text{sk-aXa}}(\mathcal{A}) := |\Pr[\text{sk-aXa}_{\Pi, \Sigma, 1}(\mathcal{A}) = 1] - \Pr[\text{sk-aXa}_{\Pi, \Sigma, 0}(\mathcal{A}) = 1]|$$

$\text{sk-aXa}_{\Pi, \Sigma, b}(\mathcal{A})$:	$\text{CHAL}(m, \hat{m}_0, \hat{m}_1)$
1 : $(pk, sk, sdk, rdk) \leftarrow \text{aKGen}(1^\lambda)$	1 : if $(ct^* \neq \perp) \vee (\hat{m}_0 \neq \hat{m}_1)$:
2 : $ct^* \leftarrow \perp$	2 : return $\perp$
3 : return $\mathcal{A}^{\text{AENC}, \text{CHAL}}(pk, sk)$	3 : $ct^* \leftarrow \text{aEnc}(pk, sdk, m, \hat{m}_b)$
4 : return $\mathcal{A}^{\text{AENC}, \text{CHAL}, \text{ADEC}}(pk, sk)$	4 : return ct^*
$\text{AENC}(m, \hat{m})$	$\text{ADEC}(ct)$
1 : return $\text{aEnc}(pk, sdk, m, \hat{m})$	1 : if $ct = ct^*$: return $\perp$
	2 : return $\text{aDec}(sk, rdk, ct)$

Fig. 26. sk-aXa security game for asymmetric AME scheme $\text{AAME} = (\Pi, \Sigma)$ for $X \in \{\text{CPA}, \text{CCA}\}$. Boxed code is only relevant in the sk-aCPAa game. Highlighted code is only relevant in the sk-aCCAa game.

is negligible in λ , where the experiment $\text{sk-aXa}_{\Pi, \Sigma, b}(\mathcal{A})$ for $b \in \{0, 1\}$ is defined in Fig. 26.

Theorem 27 (sk-dualCPA $\Rightarrow$ sk-aCPAa, and sk-dualCCA $\Rightarrow$ sk-aCCAa in AAME). Let $\text{AAME} = (\Pi, \Sigma)$ be an AAME scheme. If AAME is sk-dualCPA-secure, then it is also sk-aCPAa-secure. If AAME is sk-dualCCA-secure, then it is also sk-aCCAa-secure.

The proof is the same as in Theorem 8 and Theorem 17 and we omit here.

D.2 Security of AAME against the Anamorphic Sender

In the asymmetric setting, the double key is decomposed into the sender double key sdk and the receiver double key rdk , and the anamorphic sender has access to sdk only while rdk is kept private. Due to this, the security notions against the anamorphic sender in the asymmetric setting are weaker than those in the symmetric setting.

We first define the security of m in normal ciphertexts.

Definition 30 (sdk-CPA-AM/sdk-CCA-AM Security of Asymmetric AME). An AAME scheme $\text{AAME} = (\Pi, \Sigma)$ is sk-X-AM-secure for $X \in \{\text{CPA}, \text{CCA}\}$, if, for every PPT adversary $\mathcal{A}$, the advantage

$$\text{Adv}_{\Pi, \Sigma}^{\text{sdk-X-AM}}(\mathcal{A}) := |\Pr[\text{sdk-X-AM}_{\Pi, \Sigma, 1}(\mathcal{A}) = 1] - \Pr[\text{sdk-X-AM}_{\Pi, \Sigma, 0}(\mathcal{A}) = 1]|$$

is negligible in λ , where the experiment $\text{sdk-X-AM}_{\Pi, \Sigma, b}(\mathcal{A})$ for $b \in \{0, 1\}$ is defined in Fig. 27.

Now we define the security of m (and/or) $\hat{m}$ anamorphic ciphertexts.

sdk-X-AM $_{\Pi, \Sigma, b}(\mathcal{A})$:	CHAL(m_0, m_1)
1 : $(pk, sk, sdk, rdk) \leftarrow \text{aKGen}(1^\lambda)$	1 : if $ct^* \neq \perp \vee (m_0 \neq m_1)$: return $\perp$
2 : $ct^* \leftarrow \perp$	2 : $ct^* \leftarrow \text{Enc}(pk, m_b)$
3 : return $\mathcal{A}^{\text{CHAL}}(pk, sdk)$	3 : return ct^*
4 : return $\mathcal{A}^{\text{CHAL}, \text{ADEC}, \text{DEC}}(pk, sdk)$	<u>DEC(ct)</u>
<u>ADEC(ct)</u>	1 : if $ct = ct^*$: return $\perp$
1 : return $\text{aDec}(sk, rdk, ct)$	2 : return $\text{Dec}(sk, ct)$

Fig. 27. sdk-X-AM security game for asymmetric AME scheme $\text{AAME} = (\Pi, \Sigma)$ for $X \in \{\text{CPA}, \text{CCA}\}$. Boxed code is only relevant in the sdk-CPA-AM game. Highlighted code is only relevant in the sdk-CCA-AM game.

Definition 31 (sdk-aCPAn/sdk-aCCAn Security of Asymmetric AME [8]). An AAME scheme $\text{AAME} = (\Pi, \Sigma)$ is sk-aXn-secure for $X \in \{\text{CPA}, \text{CCA}\}$, if, for every PPT adversary $\mathcal{A}$, the advantage

$$\text{Adv}_{\Pi, \Sigma}^{\text{sdk-aXn}}(\mathcal{A}) := |\Pr[\text{sdk-aXn}_{\Pi, \Sigma, 1}(\mathcal{A}) = 1] - \Pr[\text{sdk-aXn}_{\Pi, \Sigma, 0}(\mathcal{A}) = 1]|$$

is negligible in λ , where the experiment $\text{sdk-aXn}_{\Pi, \Sigma, b}(\mathcal{A})$ for $b \in \{0, 1\}$ is defined in Fig. 28.

sdk-aXn $_{\Pi, \Sigma, b}(\mathcal{A})$:	CHAL($m_0, m_1, \hat{m}$)
1 : $(pk, sk, sdk, rdk) \leftarrow \text{aKGen}(1^\lambda)$	1 : if $ct^* \neq \perp \vee (m_0 \neq m_1)$: return $\perp$
2 : $ct^* \leftarrow \perp$	2 : $ct^* \leftarrow \text{aEnc}(pk, sdk, m_b, \hat{m})$
3 : return $\mathcal{A}^{\text{CHAL}}(pk, sdk)$	3 : return ct^*
4 : return $\mathcal{A}^{\text{CHAL}, \text{ADEC}, \text{DEC}}(pk, sdk)$	<u>DEC(ct)</u>
<u>ADEC(ct)</u>	1 : if $ct = ct^*$: return $\perp$
1 : return $\text{aDec}(sk, rdk, ct)$	2 : return $\text{Dec}(sk, ct)$

Fig. 28. sdk-aXn security game for asymmetric AME scheme $\text{AAME} = (\Pi, \Sigma)$ for $X \in \{\text{CPA}, \text{CCA}\}$. Boxed code is only relevant in the sdk-aCPAn game. Highlighted code is only relevant in the sdk-aCCAn game.

Definition 32 (sdk-aCPAa/sdk-aCCAa Security of Asymmetric AME). An AAME scheme $\text{AAME} = (\Pi, \Sigma)$ is sk-aXa-secure for $X \in \{\text{CPA},$

CCA}, if, for every PPT adversary $\mathcal{A}$, the advantage

$$\text{Adv}_{\Pi, \Sigma}^{\text{sdk-axa}}(\mathcal{A}) := |\Pr[\text{sdk-aXa}_{\Pi, \Sigma, 1}(\mathcal{A}) = 1] - \Pr[\text{sdk-aXa}_{\Pi, \Sigma, 0}(\mathcal{A}) = 1]|$$

is negligible in λ , where the experiment $\text{sdk-aXa}_{\Pi, \Sigma, b}(\mathcal{A})$ for $b \in \{0, 1\}$ is defined in Fig. 29.

$\text{sdk-aXa}_{\Pi, \Sigma, b}(\mathcal{A})$:	$\text{CHAL}(m, \hat{m}_0, \hat{m}_1)$
1 : $(pk, sk, \text{sdk}, \text{rdk}) \leftarrow \text{aKGen}(1^\lambda)$	1 : if $\text{ct}^* \neq \perp \vee (\hat{m}_0 \neq \hat{m}_1)$: return $\perp$
2 : $\text{ct}^* \leftarrow \perp$	2 : $\text{ct}^* \leftarrow \text{aEnc}(pk, \text{sdk}, m, \hat{m}_b)$
3 : return $\mathcal{A}^{\text{CHAL}}(pk, \text{sdk})$	3 : return ct^*
4 : return $\mathcal{A}^{\text{CHAL}, \text{ADec}, \text{Dec}}(pk, \text{sdk})$	$\text{ADec}(\text{ct})$
$\text{Dec}(\text{ct})$	1 : if $\text{ct} = \text{ct}^*$: return $\perp$
1 : return $\text{Dec}(sk, \text{ct})$	2 : return $\text{aDec}(sk, \text{rdk}, \text{ct})$

Fig. 29. sdk-aXa security game for asymmetric AME scheme $\text{AAME} = (\Pi, \Sigma)$ for $X \in \{\text{CPA}, \text{CCA}\}$. Boxed code is only relevant in the sdk-aCPAa game. Highlighted code is only relevant in the sdk-aCCAa game.

Definition 33 (sdk-aCPA+/sdk-aCCA+ Security of Asymmetric AME). An AAME scheme $\text{AAME} = (\Pi, \Sigma)$ is sk-aX+ -secure for $X \in \{\text{CPA}, \text{CCA}\}$, if, for every PPT adversary $\mathcal{A}$, the advantage

$$\text{Adv}_{\Pi, \Sigma}^{\text{sdk-ax+}}(\mathcal{A}) := |\Pr[\text{sdk-aX+}_{\Pi, \Sigma, 1}(\mathcal{A}) = 1] - \Pr[\text{sdk-aX+}_{\Pi, \Sigma, 0}(\mathcal{A}) = 1]|$$

is negligible in λ , where the experiment $\text{sdk-aX+}_{\Pi, \Sigma, b}(\mathcal{A})$ for $b \in \{0, 1\}$ is defined in Fig. 30.

All relationships in the last two sections apply in the asymmetric setting, and the proofs are similar except that dk is replaced with sdk here. Below, we formally write the theorems down but omit the proofs due to their similarity with the analogous symmetric AME proofs.

Theorem 28 (sdk-aCPAn ($\wedge$ sk-dualCPA) $\nRightarrow$ sdk-aCPA+, and sdk-aCCAn ($\wedge$ sk-dualCCA) $\nRightarrow$ sdk-aCCA+ in AAME). For an AAME scheme $\text{AAME} = (\Pi, \Sigma)$, sdk-aCPAn security and sk-dualCPA security together do not imply sdk-aCPA+ security, and sdk-aCCAn security and sk-dualCCA security together do not imply sdk-aCCA+ security.

Theorem 29 (sdk-aCPAa ($\wedge$ sk-dualCPA) $\nRightarrow$ sdk-aCPA+, and sdk-aCCAa ($\wedge$ sk-dualCCA) $\nRightarrow$ sdk-aCCA+ in AAME). For an AAME scheme $\text{AAME} = (\Pi, \Sigma)$, sdk-aCPAa security and sk-dualCPA security together do not imply sdk-aCPA+ security, and sdk-aCCAa security and sk-dualCCA security together do not imply sdk-aCCA+ security.

sdk-aX+ $_{\Pi, \Sigma, b}(\mathcal{A})$:	CHAL($m_0, m_1 \hat{m}_0, \hat{m}_1$)
1 : (pk, sk, sdk, rdk) $\leftarrow$ aKGen(1^λ)	1 : if $ct^* \neq \perp \vee (m_0 \neq m_1) \vee (\hat{m}_0 \neq \hat{m}_1)$:
2 : $ct^* \leftarrow \perp$	2 : return $\perp$
3 : return $\mathcal{A}^{\text{CHAL}}(\text{pk}, \text{sdk})$	3 : $ct^* \leftarrow \text{aEnc}(\text{pk}, \text{sdk}, m_b, \hat{m}_b)$
4 : return $\mathcal{A}^{\text{CHAL}, \text{ADec}, \text{Dec}}(\text{pk}, \text{sdk})$	4 : return ct^*
DEC(ct)	ADec(ct)
1 : if $ct = ct^*$: return $\perp$	1 : if $ct = ct^*$: return $\perp$
2 : return Dec(sk, ct)	2 : return aDec(sk, rdk, ct)

Fig. 30. sdk-aX+ security game for asymmetric AME scheme AAME = (Π, Σ) for $X \in \{\text{CPA}, \text{CCA}\}$. Boxed code is only relevant in the sdk-aCPA+ game. Highlighted code is only relevant in the sdk-aCCA+ game.

Theorem 30 (sdk-aCPA($n/a/+$) $\nRightarrow$ sk-aCPAa, and sdk-aCCA($n/a/+$) $\nRightarrow$ sk-aCCAa in AAME). For an AAME scheme AAME = (Π, Σ) , sdk-aCPA($n/a/+$) does not imply sk-aCPAa, and vice versa. Moreover, sdk-aCCA($n/a/+$) does not imply sk-aCCAa, and vice versa.

Theorem 31 (sdk-CPA-AM $(\wedge$ sk-dualCPA) $\nRightarrow$ sdk-aCPAa $(\wedge$ sk-dualCPA), and sdk-CCA-AM $(\wedge$ sk-dualCCA) $\nRightarrow$ sdk-aCCAa $(\wedge$ sk-dualCCA) in AAME). For an AAME scheme AAME = (Π, Σ) , sdk-CPA-AM security does not imply dk-aCPAa security, and vice versa. Moreover, sdk-CCA-AM security does not imply dk-aCCAa security, and vice versa.

Theorem 32 (sdk-aCPAn $\nRightarrow$ sdk-CPA-AM, and sdk-aCCAn $\nRightarrow$ sdk-CCA-AM in AAME). For an AAME scheme AAME = (Π, Σ) , sdk-aCPAn security does not imply sdk-CPA-AM security, and sdk-aCCAn security does not imply sdk-CCA-AM security.

Theorem 33 (sdk-CPA-AM $(\wedge$ sk-dualCPA) $\nRightarrow$ sdk-aCPA($n/+$), and sdk-CCA-AM $(\wedge$ sk-dualCCA) $\nRightarrow$ sdk-aCCA($n/+$) in AAME). For an AAME scheme AAME = (Π, Σ) , sdk-CPA-AM security and sk-dualCPA security do not imply sdk-aCPA($n/+$) security, and sdk-CCA-AM security and sk-dualCCA security do not imply sdk-aCCA($n/+$) security.

Theorem 34 (sdk-CPA-AM $\wedge$ sk-dualCPA $\Rightarrow$ IND-CPA, and sdk-CCA-AM $\wedge$ sk-dualCCA $\Rightarrow$ IND-CCA, but sdk-CPA-AM $\nRightarrow$ IND-CPA $(\wedge$ sk-dualCPA), and sdk-CCA-AM $\nRightarrow$ IND-CCA $(\wedge$ sk-dualCCA)). For an AAME scheme AAME = (Π, Σ) , sdk-CPA-AM security and sk-dualCPA security together imply IND-CPA security, and sdk-CCA-AM security and sk-dualCCA security together imply IND-CCA security. However, IND-CPA security and sk-dualCPA do not imply sdk-CPA-AM security, and IND-CCA security and sk-dualCCA security do not imply sdk-CCA-AM security.

Theorem 35 ($\text{sdk-aCPA}(n/+) \wedge \text{sk-dualCPA} \Rightarrow \text{IND-CPA}$, and $\text{sdk-aCCA}(n/+) \wedge \text{sk-dualCCA} \Rightarrow \text{IND-CCA}$, but $\text{sdk-aCPA}(n/+) \not\Leftarrow \text{IND-CPA} (\wedge \text{sk-dualCPA})$, and $\text{sdk-aCCA}(n/+) \not\Leftarrow \text{IND-CCA} (\wedge \text{sk-dualCCA})$). For an AAME scheme $\text{AAME} = (\Pi, \Sigma)$, $\text{sdk-aCPA}(n/+)$ security and sk-dualCPA security together imply IND-CPA security, and $\text{sdk-aCCA}(n/+)$ security and sk-dualCCA security together imply IND-CCA security. However, IND-CPA security and sk-dualCPA do not imply $\text{sdk-aCPA}(n/+)$ security, and IND-CCA security and sk-dualCCA security do not imply $\text{sdk-aCCA}(n/+)$ security.

Theorem 36 ($\text{IND-CPA} (\wedge \text{sk-dualCPA}) \not\Leftarrow \text{sdk-aCPAa} (\wedge \text{sk-dualCPA})$, and $\text{IND-CCA} (\wedge \text{sk-dualCCA}) \not\Leftarrow \text{sdk-aCCAa} (\wedge \text{sk-dualCCA})$). For an sk-dualCPA -secure AAME scheme $\text{AAME} = (\Pi, \Sigma)$, IND-CPA security does not imply sdk-aCPAa security, and vice versa. Moreover, for an sk-dualCCA -secure AAME scheme, IND-CCA security does not imply sdk-aCCAa security, and vice versa.

D.3 Security Notions against Collusion and Relationships

In this subsection we supply additional definitions and proofs for the security against the collusion of the dictator and the anamorphic sender.

Definition 34 (sk-sdk-aCPAa [8]/ sk-sdk-aCCAa **Security of Asymmetric AME**). An AAME scheme $\text{AAME} = (\Pi, \Sigma)$ is sk-sdk-aXa -secure for $X \in \{\text{CPA}, \text{CCA}\}$, if, for every PPT adversary $\mathcal{A}$, the advantage

$$\text{Adv}_{\Pi, \Sigma}^{\text{sk-sdk-axa}}(\mathcal{A}) := |\Pr[\text{sk-sdk-aXa}_{\Pi, \Sigma, 1}(\mathcal{A}) = 1] - \Pr[\text{sk-sdk-aXa}_{\Pi, \Sigma, 0}(\mathcal{A}) = 1]|$$

is negligible in λ , where the experiment $\text{sk-sdk-aXa}_{\Pi, \Sigma, b}(\mathcal{A})$ for $b \in \{0, 1\}$ is defined in Fig. 31.

$\text{sk-sdk-aXa}_{\Pi, \Sigma, b}(\mathcal{A})$:	$\text{CHAL}(m, \hat{m}_0, \hat{m}_1)$
1 : $(pk, sk, sdk, rdk) \leftarrow \text{aKGen}(1^\lambda)$	1 : if $ct^* \neq \perp \vee (\hat{m}_0 \neq \hat{m}_1)$: return $\perp$
2 : $ct^* \leftarrow \perp$	2 : $ct^* \leftarrow \text{aEnc}(pk, sdk, m, \hat{m}_b)$
3 : return $\mathcal{A}^{\text{CHAL}}(pk, sk, sdk)$	3 : return ct^*
4 : return $\mathcal{A}^{\text{CHAL}, \text{ADEC}}(pk, sk, sdk)$	ADEC(ct)
	1 : if $ct = ct^*$: return $\perp$
	2 : return $\text{aDec}(sk, rdk, ct)$

Fig. 31. sk-sdk-aXa security game for asymmetric AME scheme $\text{AAME} = (\Pi, \Sigma)$ for $X \in \{\text{CPA}, \text{CCA}\}$. Boxed code is only relevant in the sk-sdk-aCPAa game. Highlighted code is only relevant in the sk-sdk-aCCAa game.

We argue that sk-sdk-dualCPA implies sk-sdk-aCPAa , and sk-sdk-dualCCA implies sk-sdk-aCCAa .

Theorem 37 ($\text{sk-sdk-dualCPA} \Rightarrow \text{sk-sdk-aCPAa}$, and $\text{sk-sdk-dualCCA} \Rightarrow \text{sk-sdk-aCCAa}$). *Let $\text{AAME} = (\Pi, \Sigma)$ be an asymmetric AME scheme. If AAME is sk-sdk-dualCPA secure, then it is also sk-sdk-aCPAa -secure. If AAME is sk-sdk-dualCCA secure, then it is also sk-sdk-aCCAa -secure.*

Proof. We prove the theorem in the CPA setting and the CCA setting is analogous. Let $\mathcal{A}$ be an adversary against the sk-sdk-aCPAa security of an asymmetric AME scheme. Consider the hybrid game $\text{Hybrid}_{\Pi, \Sigma}(\mathcal{A})$ in which the adversary gets pk, sdk , inputs $(m, \hat{m}_0, \hat{m}_1)$ as the challenge query and obtains $\text{Enc}(\text{pk}, m)$ as the challenge ciphertext. By sk-sdk-dualCPA security of AME, $\text{Hybrid}_{\Pi, \Sigma}(\mathcal{A})$ is indistinguishable to the experiment $\text{sk-sdk-aCPA}_{\Pi, \Sigma, b}(\mathcal{A})$ for both $b = 0$ and $b = 1$, which shows the indistinguishability of $\text{sk-sdk-aCPA}_{\Pi, \Sigma, 1}(\mathcal{A})$ and $\text{sk-sdk-aCPA}_{\Pi, \Sigma, 0}(\mathcal{A})$. $\square$

Now we investigate the relationships among sk-sdk-dualCPA , sk-sdk-aCPAa , and other security notions. The results also hold in the CCA setting.

It is easy to see that sk-sdk-dualCPA is strictly stronger than sk-dualCPA , and similarly sk-sdk-aCPAa is strictly stronger than sk-aCPAa due to the additional information of sdk provided to the adversary.¹⁸ Then, what about the relationship between sk-dualCPA and sk-sdk-aCPAa ? In the following theorem, we will see that those two notions are incomparable.

Theorem 38 ($\text{sk-dualCPA} \not\Rightarrow \text{sk-sdk-aCPAa}$). *For an asymmetric AME scheme $\text{AAME} = (\Pi, \Sigma)$, sk-dualCPA does not imply sk-sdk-aCPAa , and vice versa.*

Proof. The proof of one direction, $\text{sk-dualCPA} \not\Rightarrow \text{sk-sdk-aCPAa}$ is addressed by a symmetric AME scheme (a specific case of asymmetric AME when $\text{sdk} = \text{rdk}$), where holding both sk and $\text{sdk} = \text{rdk}$ enables one to totally read both the normal message and the anamorphic message in a ciphertext.

To prove the other direction, we construct an aAME scheme $\widetilde{\text{AAME}}$ from an sk-sdk-aCPAa -secure asymmetric AME scheme AAME as follows.

- The key generation algorithm and the anamorphic key generation algorithm are the same as those of $\widetilde{\text{AAME}}$.
- The encryption algorithm $\text{Enc}(\text{pk}, m)$ returns $\widetilde{\text{AAME}}.\text{Enc}(\text{pk}, (m||0))$.¹⁹
- The anamorphic algorithm $\text{aEnc}(\text{pk}, \text{sdk}, m)$ returns $\widetilde{\text{AAME}}.\text{Enc}(\text{pk}, \text{sdk}, (m||1), \hat{m})$.

¹⁸ Note that to formally prove it, we need to first introduce a hybrid game which is the same as $\text{sk-dualCPA}_{\Pi, \Sigma, 0}(\mathcal{A})$ (the normal mode) except that $\text{KGen}(1^\lambda)$ is replaced with $\text{aKGen}(1^\lambda)$, see Lemma 1.

¹⁹ For the simplicity of the proof we assume the message space of $\widetilde{\text{AAME}}$ is of length $|m| + 1$.

Obviously, once a ciphertext from the construction is decrypted, one must know whether it comes from the normal mode or anamorphic mode. Hence, even if $\widetilde{\text{AAME}}$ is sk-sdk-aCPAa, AAME is not sk-dualCPA. $\square$

Theorem 39 (sk-dualCCA $\nRightarrow$ sk-sdk-aCCAa). *For an asymmetric AME scheme $\text{AAME} = (\Pi, \Sigma)$, sk-dualCCA does not imply sk-sdk-aCCAa, and vice versa.*

Relationships with Security Notions against the Anamorphic Sender.

Now we investigate the relationships between the two new notions (sk-sdk-dualCPA and sk-sdk-aCPAa) and security notions against the anamorphic sender (sdk-CPA-AM and sdk-aCPA(n/a/+)).

Theorem 40 (sdk-CPA-AM / sdk-aCPAn / sdk-aCPA+ $\nRightarrow$ sk-sdk-aCPAa). *For an asymmetric AME scheme $\text{AAME} = (\Pi, \Sigma)$, sdk-CPA-AM, sdk-aCPAn, or sdk-aCPA+ do not imply sk-sdk-aCPAa.*

Proof. This can be easily seen by seeing the special case $\text{rdk} = \text{sdk}$. In this case, even if sdk-CPA-AM (or sdk-aCPAn or sdk-aCPA+) holds, it is trivially not sk-sdk-aCPAa because an adversary has both sk and $\text{rdk} = \text{sdk}$ so that it can freely run anamorphic decryption. $\square$

Theorem 41 (sdk-CCA-AM / sdk-aCCAn / sdk-aCCA+ $\nRightarrow$ sk-sdk-aCCAa). *For an asymmetric AME scheme $\text{AAME} = (\Pi, \Sigma)$, sdk-CCA-AM, sdk-aCCAn, or sdk-aCCA+ do not imply sk-sdk-aCCAa.*

Theorem 42 (sdk-CPA-AM / sdk-aCPAn / sdk-aCPA+ $\nRightarrow$ sk-sdk-dualCPA). *For an asymmetric AME scheme $\text{AAME} = (\Pi, \Sigma)$, sk-sdk-dualCPA does not imply sdk-CPA-AM, sdk-aCPAn, or sdk-aCPA+.*

Proof. The proof can be done by constructing a counterexample. Let Π be an PR-CT secure PKE scheme with public key sdk and secret key rdk . We construct an AME scheme where the normal encryption returns $(\mathbf{m}||\text{str})$ with str some random string, and the anamorphic encryption returns $(\mathbf{m}||\Pi.\text{Enc}(\text{sdk}, \hat{\mathbf{m}}))$. The construction is sk-sdk-dualCPA secure due to the PR-CT security of Π . However, it is trivially insecure as sdk-CPA-AM, sdk-aCPAn, or sdk-aCPA+. $\square$

Theorem 43 (sdk-CCA-AM / sdk-aCCAn / sdk-aCCA+ $\nRightarrow$ sk-sdk-dualCCA). *For an asymmetric AME scheme $\text{AAME} = (\Pi, \Sigma)$, sk-sdk-dualCPA does not imply sdk-CPA-AM, sdk-aCPAn, or sdk-aCPA+.*

Proof. In the CCA setting, the proof can be done by constructing a counterexample of AAME scheme where the normal encryption returns $(\mathbf{m}||\text{str}_1||\text{str}_2)$ with $\text{str}_1, \text{str}_2$ some random strings, and the anamorphic encryption returns $(\mathbf{m}||\Pi.\text{Enc}(\text{sdk}, \hat{\mathbf{m}}; r)||H(\mathbf{m}, \hat{\mathbf{m}}, r))$, and $H(\cdot)$ is a random oracle. $\square$

Since sk-sdk-dualCPA (resp., sk-sdk-dualCCA) is strictly stronger than sk-sdk-aCPAa (resp., sk-sdk-aCCAA) by Theorem 37, we immediately obtain the following two corollaries.

Corollary 3 ($\text{sdk-CPA-AM} / \text{sdk-aCPAn} / \text{sdk-aCPA+} \not\Leftarrow \text{sk-sdk-dualCPA}$, and $\text{sdk-CCA-AM} / \text{sdk-aCCAn} / \text{sdk-aCCA+} \not\Leftarrow \text{sk-sdk-dualCCA}$). *For an asymmetric AME scheme $\text{AME} = (\Pi, \Sigma)$, sdk-CPA-AM , sdk-aCPAn , or sdk-aCPA+ do not imply sk-sdk-dualCPA , and vice versa. Moreover, sdk-CCA-AM , sdk-aCCAn , or sdk-aCCA+ do not imply sk-sdk-dualCCA , and vice versa.*

Corollary 4 ($\text{sdk-CPA-AM} / \text{sdk-aCPAn} / \text{sdk-aCPA+} \not\Leftarrow \text{sk-sdk-aCPAa}$, and $\text{sdk-CCA-AM} / \text{sdk-aCCAn} / \text{sdk-aCCA+} \not\Leftarrow \text{sk-sdk-aCCAA}$). *For an asymmetric AME scheme $\text{AME} = (\Pi, \Sigma)$, sdk-CPA-AM , sdk-aCPAn , or sdk-aCPA+ do not imply sk-sdk-aCPAa , and vice versa. Moreover, sdk-CCA-AM , sdk-aCCAn , or sdk-aCCA+ do not imply sk-sdk-aCCAA , and vice versa.*

E Further Discussion

Additional Comparison with [17]. At the end of Section 1.1, we provided some comparison with the recent concurrent work of Jaeger and Stracovsky [17]. We provide some additional comparison here.

The authors note that it is not philosophically clear how to define sk-dualCCA . Their reasoning is as follows: it is not clear how the decryption oracle should be defined in the ‘normal’ world when there is no double key. By considering AME schemes with explicit rejection in decryption, we believe that our definition (Definition 7) is appropriate.

By contrast to our work, the authors consider *stateful* AME schemes, i.e., where anamorphic encryption algorithms (and signatures in their case) additionally take a state as input which is then updated and output. They however do not consider asymmetric AME as we do.

Their notion of RUF-CAMA security for signatures roughly corresponds to ROB-CT+ security, except that the adversary is given the double key dk . For encryption, this does not make sense (nor does ROB-PT security), since anamorphic encryption takes the double key as input, and thus the adversary can trivially forge a ciphertext and win. The authors do not consider additional security notions where the double key is leaked to the adversary (security against the anamorphic sender); we consider multiple.

Security in the Semi-Adaptive Setting. Recently, Catalano, Giunta, and Migliaro [9] introduced so-called semi-adaptive security, where the adversary is restricted to perform all oracle queries before obtaining sk . The semi-adaptive notion is proposed to circumvent the impossibility result of black-box constructing AME (from rejection sampling [24]) in order to provide some positive results. We emphasize that the semi-adaptive security in [9] is strictly weaker than the

basic sk-dualCPA notion considered in this paper (and also all other works on AME [24,8,1,20,25,28]).

All notions in our work consider the adaptive setting, where the adversary can query oracles adaptively after observing sk and/or dk . Additionally, all the (non-)implication relationships proven in this work also hold in the semi-adaptive setting, due to the independence of challenge queries and sk/dk in the proofs.

Issues in Sharing the Double Key Privately. A basic assumption in anamorphic encryption is that the double key (or the sender double key) is privately shared between the anamorphic sender and the receiver. The issue of sharing the double key secretly was recently studied by Wang et al. in [28], where a so-called anamorphic authenticated key exchange protocol was introduced to allow two parties to assign a double key under the surveillance of the dictator. Additionally, a public-key anamorphic scheme [10] can also facilitate the distribution of a double key, since the anamorphic sender is able to do anamorphic encryption with only the public key. Therefore, a fresh double key can be carried on as an anamorphic message and transmitted to the receiver secretly.

Issues in Fake Anamorphic Senders. As we discussed in the introduction, the sk-sdk-dualCPA and sk-sdk-dualCCA security notions are motivated by the scenario in which the anamorphic sender and the dictator collude. One may raise the following question:

What if one can generate a fake sender double key to impersonate the anamorphic sender? Could it be harmful if the one hands over this fake key to the dictator?

This is actually a desirable property since it means that the dictator cannot distinguish an anamorphic ciphertext and a normal ciphertext even in the presence of sdk and a fake one, respectively. If it is hard to link a fake key and a ciphertext, whenever sdk is revealed to the dictator, it might imply the ciphertext is indeed anamorphic and the dictator may know this. But if it is easy to link a ciphertext with a fake key in general, then the dictator cannot know whether a given ciphertext-key pair is correct or not. Hence, if a scheme has this property, the anamorphic sender and receiver enjoy one more layer of barrier from the dictatorship; even if sdk leaks, they can claim that the key is fake and they are innocent.

Sender-Anamorphic Encryption. Persiano et al. [24] proposed sender-anamorphic encryption, which allows the sender to privately send an duplicate message out when it is forced to send a “fake” message to some specified receiver. In this work we focus on the study of receiver-AME. An interesting question would be to perform a similar classification and study of sender-AME.

Table of Contents

A Unified Treatment of Anamorphic Encryption	1
<i>Wonseok Choi, Daniel Collins, Xiangyu Liu, and Vassilis Zikas</i>	
1 Introduction.....	1
1.1 Contributions and Technical Overview	3
1.2 Roadmap.....	7
2 Motivation and Overview	7
3 Preliminaries	11
4 Anamorphic Encryption: Syntax, Security, and More	11
4.1 Security Notions against the Dictator	13
4.2 Security Notions against the Anamorphic Sender	14
5 Security of Anamorphic Encryption in the CCA Setting	18
5.1 Robustness Notions.....	18
5.2 Security against the Dictator in the CCA Setting.....	19
5.3 Security against the Anamorphic Sender	21
5.4 Randomness-Recovering PKE: Achieving All Symmetric Security Notions	21
6 Security of Asymmetric Anamorphic Encryption	26
6.1 Security against the Collusion of the Dictator and the Anamorphic Sender in the Asymmetric Setting.....	27
6.2 AAME Schemes Satisfying All Asymmetric Security Notions	28
A Additional Preliminaries	33
A.1 Public-Key Encryption	33
A.2 Symmetric Encryption	34
A.3 Authenticated Encryption	35
A.4 Pseudorandom Functions	36
A.5 Ideal Ciphers	36
B Additional Results in the CPA Setting.....	36
C Additional Results in the CCA Setting	43
D Additional Results for Asymmetric AME.....	53
D.1 Security of AAME against the Dictator	53
D.2 Security of AAME against the Anamorphic Sender	54
D.3 Security Notions against Collusion and Relationships	58
E Further Discussion	61