From Rerandtopia to Interceptopia, the Anamorphic Encryption Saga Rises

Vincenzo Botta[1⋆], Dario Catalano[2], Emanuele Giunta[3], Francesco Migliaro[4], Daniele Venturi[5], and Ivan Visconti[5]

[1] Independent researcher
botta.vin@gmail.com
[2] Dipartimento di Matematica e Informatica, Università di Catania, Catania, Italy.
catalano@dmi.unict.it
[3] ETH Zurich, Zurich, Switzerland.
emanuele.giunta@inf.ethz.ch
[4] IRIF, CNRS, Université Paris Cité, Paris, France.
migliaro@irif.fr
[5] Sapienza University of Rome, Rome, Italy.
venturi@di.uniroma1.it, visconti@diag.uniroma1.it

Abstract. Nowadays, governments are world-wide pushing towards building infrastructures to intercept, decrypt and prevent communications among citizens with the goal of catching criminals.
The recent notion of anamorphic encryption proposed by Persiano et al. [Eurocrypt 2022] faces the risks of abuses derived from such infrastructures that could be maliciously leveraged to realize the phantom menace of large-scale mass-surveillance programs.
Several recent papers showed positive results on the existence of anamorphic encryption schemes, mostly confined to basic settings.
In this work we consider extreme scenarios where in addition to obtaining secret keys, the authority actively tries to sanitize ciphertexts removing covert communication.
Despite anamorphic encryption might look impossible to achieve in the above settings, we give new definitions and somewhat surprising positive results in two scenarios: Rerandtopia and Interceptopia. Our findings highlight the need to standardize new encryption schemes to counteract evolving threats.
Our main construction consists of two layers of encryption. Interestingly, when carefully instantiated, our scheme achieves a notion of rerandomizable CCA encryption that outperforms the state of the art in terms of assumptions and efficiency.

⋆ Work done while at Sapienza University of Rome, Rome, Italy.

Table of Contents

1 Introduction **3**
- 1.1 Our Contributions 4
- 1.2 Technical Overview 5
- 1.3 Related Works 7

2 Preliminaries **7**
- 2.1 Symmetric Encryption with Pseudorandom Ciphertext 8
- 2.2 Public Key Encryption 9
- 2.3 Deterministic PKE 11
- 2.4 Anamorphic Encryption 11

3 Re-randomization Resistant Anamorphic Encryption **13**
- 3.1 Preliminary results on AE 14
- 3.2 Generic Construction of Re-randomization Resistant AE 16
- 3.3 On the Existence of anam-NM-CPA AE 20

4 Deterministic Anamorphic Encryption **21**

5 Black-box Re-randomizable PKE **25**
- 5.1 Two-Layer Construction 25
- 5.2 Instantiations 28

A Additional Definitions **32**
- A.1 IND-CCA2 Secure Encryption 32
- A.2 Non-Malleable Encryption 32
- A.3 Robustness of AE 33

1 Introduction

A new hope. The notion of (receiver) Anamorphic Encryption (AE) [32] enables private communication in adversarial environments where users' secret decryption keys may be compromised. Such situations can occur, for example, under authoritarian regimes where individuals are subjected to strict monitoring and may be forced to hand over their private keys. At a high level, AE attains this seemingly paradoxical goal by offering two operating modes: *regular* and *anamorphic*. In regular mode, the system functions as a standard public-key encryption scheme. In anamorphic mode, however, a public key (apk) is associated to *two* secret keys: a standard-looking one (ask) and a covert one, called the "double key" (dk). Bob secretly shares dk with Alice while publishing apk as his public key. If compelled by an adversary to reveal his secret key, Bob only discloses ask.

A key property of AE is that the pair $(\mathsf{apk}, \mathsf{ask})$ remains fully compatible with the underlying regular encryption scheme. However, Alice can employ dk as a symmetric key to embed an *additional* hidden message into the ciphertext, which stays concealed even when ask is known. Thus, in anamorphic mode, the scheme allows the encryption of two messages: a regular message m, intended for adversarial inspection via ask, and a covert message $\hat{m}$, recoverable only with dk. The central security requirement is that anamorphic ciphertexts must be indistinguishable from regular ones.

Over the last few years several works studied AE, across multiple research directions. Initial works focused on demonstrating that *existing* (and possibly widely deployed) schemes possess anamorphic properties (e.g., [32, 27, 2, 39, 10]). Other works considered refined definitions (e.g. [2, 10, 33]), inherent limitations (e.g. [11, 12, 9, 19, 1]) and connections with other primitives (e.g. [39, 9]). In principle, the adversarial authority (e.g., the dictator of an empire) aware of main techniques used to encode secret messages in ciphertexts, could resort to so-called anamorphic-resistant encryption (ARE) [12, 9, 19, 1], that, as the name suggests, provably disallows any covert communication. This option, however is currently not practical though: all known AREs have some undesirable weaknesses, for example [19] requires the RO, or are too inefficient to be used in real-life applications.

The dictator strikes back. In this work, we observe that with the goal of sanitizing ciphertexts sent with schemes that are potentially anamorphic, the authority can upgrade the surveillance infrastructure as follows: while keeping the option of forcing a user to reveal the secret key, the authority also takes control of the communication infrastructure making sure that in the path from sender to receiver, there is always a node (e.g., a router, or proxy) running an algorithm aiming at sanitizing the ciphertexts. Given the structure of the Internet (i.e., the existence of several ISPs and the dynamic paths preventing single points of failure), there should be several of such nodes.

The authority can use such nodes to re-randomize the ciphertexts, forbidding those schemes that are not re-randomizable (e.g., CCA2 schemes). Given that the main approach to encode a secret message into a ciphertext consists of carefully

choosing the randomness used to encrypt, this upgraded attack of the authority is seemingly devastating. Notice that no secret is required in the nodes that perform the re-randomization and this makes the approach very appealing for the authority since delivering secret keys in multiple places exposes risks due to potential data breaches.

A more aggressive authority, might instead be willing to risk that a data breach generates a leak of the secret keys, and thus can make those nodes stronger by storing in them also the secret keys of the users. In this way a node receiving a ciphertext can be way more aggressive decrypting first the ciphertext, and then encrypting the plaintext again. This riskier attack is very effective and clearly there can not be an anamorphic encryption scheme in this stronger setting. Obviously this attack is much harder to mount since in realistic scenarios the authority gets the secret after the fact, when an investigation starts, therefore after the communication has been completed already.

One might wonder if there is still room to defeat such a stronger authority with the goal of achieving (receiver) AE even in this more challenging scenarios.

1.1 Our Contributions

Motivated by the above stronger attack scenarios that we envision, in this work we revisit the concept of anamorphic encryption to consider the stronger and seemingly realistic setting in which the authority leverages the power to decrypt users' ciphertexts (e.g., in case of criminal investigations) while also trying to contrast covert channels inside encryption.

Concretely, we study two settings.

- **Rerandtopia.** Given that AE typically uses the encryption randomness to hide covert messages, in this world the authority forbids schemes that are not rerandomizable and tries to block covert messages by using network-level firewalls that re-randomize ciphertexts before transmission. In fact, re-randomization is relatively cheap to implement, it does not require access to secret keys, and authorities can specify re-randomization procedures for each standardized encryption scheme that is allowed for public usage (of course chosen-ciphertext attacks secure encryption would be banned).
- **Interceptopia.** In this world, the authority takes a much more extreme approach to block covert communication by using network-level firewalls that are allowed to decrypt and re-encrypt each ciphertext before transmission using fresh randomness.

An intriguing question is whether some notions of anamorphic communication are still possible in Rerandtopia and Interceptopia.

Return of the Anamorpher. The main result of this paper is a positive answer to the above question. We show new constructions of AE that allow for covert communication in both Rerandtopia and Interceptopia. The construction in Rerandtopia is a two-layer encryption where the external layer allows re-randomization while the inner layer safely accommodates the anamorphic message.

In Interceptopia there is an obvious impossibility result of the original notion of anamorphic encryption. However we will still obtain a positive results circumventing the power of the dictator by transferring the anamorphic message in the actual plaintext. As such, we will entirely focus on constructing Deterministic AE, therefore limiting positive results to restricted message spaces.

We remark that prior work on anamorphic encryption considers a threat model with a limited dictator and such limitations allow to prove that some of the existing schemes are anamorphic. Instead, in our work we consider a more comprehensive threat model that includes among the adversaries a more powerful dictator that clearly defeats all known schemes. Therefore, in our work we will propose new constructions showing that even in the presence of such a stronger dictator, anamorphic encryption is possible. This can be considered as a sign that more advanced encryption schemes should be standardized, since additional properties like anamorphism are gaining increasing interest.

Re-randomizable CCA encryption. Last but not least, we connect Rerandtopia with the known concept of re-randomizable CCA encryption. Indeed, we show that when instantiating differently our two-layer encryption that defeats the dictator in Rerandtopia, the resulting encryption scheme outperforms a prior work of [21] both in terms of assumptions (in contrast to them, we do not need random oracles) and of efficiency (our ciphertexts are more compact).

1.2 Technical Overview

Re-randomization resistant AE. In Sec. 3, we consider *re-randomization resistant* AE. Intuitively, this is a kind of AE whose anamorphic properties are unaffected, even in case ciphertexts are re-randomized. In our definition, the adversary is allowed to choose both the regular and anamorphic messages to encrypt, and, upon receiving the challenge ciphertext c, the adversary (without having the secret key) should not be able to produce a different ciphertext c' that decrypts to the *same regular* message and a *different anamorphic* message, despite the encryption scheme is re-randomizable. We observe that at first sight, this seems to stop covert communication in Rerandtopia. Moreover, re-randomizing ciphertexts is just a particular way the authority would use to kill covert communication and potentially other techniques can also be used to sanitize ciphertexts.

Interestingly, we show an efficient scheme that is anamorphic secure (in the IND-CPA sense) under the standard definition, is re-randomizable, and is also re-randomization resistant. The scheme roughly works using two specific encryptions in a onion-style. First we use an AE E_1 that is non-malleable against chosen-plaintext attacks (NM-CPA), and this produces an intermediate ciphertext that can include an anamorphic message. Then we encrypt the above ci-

phertext with a re-randomizable encryption scheme E_2 with indistinguishability against chosen-plaintext attacks (IND-CPA).[6]

The intuition about the above construction works is that the NM-CPA property of the inner ciphertext protects from attack in which the adversarial re-randomizer tries to obtain a new inner ciphertext that encodes the same regular plaintext. The re-randomizability of the external encryption makes the scheme suitable for those applications (e.g., shuffles, mixers) targeting anonymity, and to deceive dictators that willing to unlink communications among dissidents.

Deterministic AE. In Sec. 4, we consider *deterministic* AE. Intuitively, this is a kind of AE in which the *regular* encryption mode is deterministic, yet for messages with high-enough min-entropy the regular mode and the deterministic mode are indistinguishable. This clearly makes covert communication possible in Interceptopia, as decrypting and re-encrypting the intercepted ciphertext produces the same result.

We realize deterministic AE as follows: in *regular mode*, we use a deterministic encryption supporting uniformly random messages; in *anamorphic mode*, we first encrypt the anamorphic message using symmetric encryption with pseudorandom ciphertexts [28], and then encrypt the resulting ciphertext using deterministic encryption. Using standard constructions of deterministic encryption, and any pseudorandom function, we thus obtain instantiations under different hardness assumptions (with or without random oracles) and with different efficiency tradeoffs.

We stress that our positive results on Deterministic AE translate directly into positive results in Interceptopia, where achieving anamorphic encryption generically is obviously impossible.

Black-box re-randomizable PKE. In Sec. 5, we apply our two-layer encryption approach in order to obtain a black-box construction of so-called *re-randomizable* PKE, which is a regular PKE whose ciphertexts can be efficiently re-randomized given the public key. This kind of PKE schemes has been studied in several previous works [23, 34, 35, 22, 21], and has various applications (e.g., for realizing so-called mix-nets). A re-randomizable PKE should satisfy two security requirements. On the one hand, re-randomized ciphertexts should be efficiently computable and indistinguishable from a fresh encryption of the underlying message (if it exists); this property is called re-randomizability under chosen-plaintext attacks (RAND-CPA).[7] On the other hand, re-randomization should be the only allowed malleability on ciphertexts; this property is called *replayable* CCA (RCCA) security.

We realize re-randomizable PKE in a black-box way as follows: first, we encrypt the message using an IND-CCA2 PKE E_1, and then we encrypt the result-

[6] Of course, for this to work the message space of E_2 needs to coincide with the ciphertext space of E_1.

[7] There is also an IND-CCA1 variant (RAND-CCA1) in which the attacker also has decryption capabilities.

ing ciphertext using a re-randomizable PKE E_2. RCCA security follows easily by IND-CCA2 security of E_1. As for RAND-CPA (resp. RAND-CCA1) security, one would hope that it suffices to assume that E_2 satisfies both IND-CPA and RAND-CPA security. However, the reduction spectacularly breaks and we were only able to make it work by assuming that E_2 satisfies IND-CCA1 security (i.e., decryption queries are allowed prior to seeing the challenge ciphertext). By taking E_1 to be fully-fledged Cramer-Shoup and E_2 to be Cramer-Shoup Lite (optimized by re-using part of the randomness to encrypt the inner ciphertext), we obtain a construction of re-randomizable PKE in the plain model under the DDH assumption, with ciphertexts consisting of 7 group elements.

1.3 Related Works

AE is related but distinct from other notions in the literature; see [32] for a comprehensive comparison. Extensions achieving stronger privacy guarantees against parties with access to dk appear in [27, 10, 14]. The notion of robustness for AE was introduced in [2] and later adapted to a different setting in [39], while a stronger notion of robustness was proposed in [19]. Limitations of AE are explored in [11, 12]. In [19] schemes matching limitations are proposed, with stronger forms of resistance developed in [9]. The connection between AE and Algorithm Substitution Attacks (ASA) [5] is highlighted in [39, 9], enabling cross-interpretation of results. In [18], AE is extended to a one-to-many setting, where different receivers can extract distinct anamorphic messages from the same ciphertext. More extreme scenarios, where encryption is banned but authentication is not, are studied in [26], introducing anamorphic signatures for covert messaging via authentication channels; further refinements appear in [24]. Finally, [38] introduces Anamorphic Key Exchange, enabling the covert sharing of a double key using standard key exchange protocols.

The notion of RCCA security was proposed by Canetti *et al.* [8] as a relaxation of CCA security. This was later adapted to consider the practically relevant case of re-randomizable encryption by Groth [23], who obtained *perfectly* re-randomizable schemes with RCCA security under the DDH assumption (against semi generic adversaries). Several other constructions were proposed afterwards [34, 35, 22, 21], trading efficiency with computational variants of re-randomizability and stronger assumptions. Previously to our work, the most efficient scheme achieved 11 group elements assuming the DDH assumption and non-programmable random oracles [21].

2 Preliminaries

$[n]$ denotes the set $\{1, \ldots, n\}$. $\lambda \in \mathbb{N}$ is the security parameter. A function $f : \mathbb{N} \to \mathbb{R}^+$ is *negligible* if it vanishes faster than the inverse of any polynomial. $\mathsf{negl}(\lambda)$ denotes a generic negligible function. Given a probabilistic Turing Machine $\mathcal{A}$ we denote $y = \mathcal{A}(x; r)$ its output on input x and random tape r. The notation $y \leftarrow^{\$} \mathcal{A}(x)$ is short for $y = \mathcal{A}(x; r)$ with r being a uniformly sampled

tape. With PPT we denote probabilistic polynomial time. With $\overset{c}{\approx}_\delta$ we denote the computationally δ-close indistinguishability, we omit δ in case of standard computational indistinguishability. Given a set S we denote by $x \leftarrow^{\$} S$ the uniformly random sampling of an element x from the set S. We write $x \leftarrow^{\$} D(S)$ to indicate that x is sampled from S according to the distribution D. We further write $X \sim D(S)$ to indicate that x is a random variable distributed over S according to D.

Unless otherwise specified, we assume *adversaries* in security definitions to be *stateful*, and procedures in a given scheme (e.g. a PKE) to be *stateless*. Also, we may omit the game in the adversary's advantage $\mathcal{A}$ when clear from context.

With ϵ we denote the empty string. Given two strings x and y, we denote with $x\|y$ their concatenation.

Definition 1. *Let X be a discrete random variable with support $\mathcal{X}$. The min-entropy of X is defined as:* $\mathrm{H}_\infty(X) = -\log\left(\max_{x_0 \in \mathcal{X}} \Pr\left[X = x_0\right]\right)$.

Definition 2. *A probability distribution D over a set S has high min-entropy if, for a random variable $X \sim D(S)$, it holds that* $\mathrm{H}_\infty(X) = \Omega(\log |S|)$.

Definition 3. *Let $\ell \in \mathbb{N}, t \in \mathbb{R}^+$. A random variable X with support $\{0,1\}^\ell$ is called a (t,ℓ)-source if* $\mathrm{H}_\infty(X) \geq t$.

2.1 Symmetric Encryption with Pseudorandom Ciphertext

A stronger security definition than IND-CPA achievable by a secret key encryption (SKE) scheme is the pseudorandomness of ciphertexts. We recall the definition of a SKE scheme with pseudorandom ciphertext from [28, 27, 26]. Let $\mathsf{prE} = (\mathsf{prE.Gen}, \mathsf{prE.Enc}, \mathsf{prE.Dec})$ be a symmetric encryption scheme with message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$. We define the game $\mathsf{PRCtG}^b_{\mathsf{prE},\mathcal{D}}(\lambda)$, for $b \in \{0,1\}$, in Fig. 1.

$\mathsf{PRCtG}^b_{\mathsf{prE},\mathcal{D}}(\lambda)$

1 : $\mathsf{sk} \leftarrow^{\$} \mathsf{prE.Gen}(\lambda)$
2 : **return** $\mathcal{D}^{\mathcal{O}pr^b(\mathsf{sk},\cdot)}(\lambda)$ where
3 : $\quad \mathcal{O}pr^0(\mathsf{sk}, m) = c \leftarrow^{\$} \mathcal{C}$
4 : $\quad \mathcal{O}pr^1(\mathsf{sk}, m) = \mathsf{prE.Enc}(\mathsf{sk}, m)$

Fig. 1. Pseudorandom ciphertexts game.

We define the advantage of an adversary $\mathcal{D}$ in distinguishing between games $\mathsf{PRCtG}^0_{\mathsf{prE},\mathcal{D}}(\lambda)$ and $\mathsf{PRCtG}^1_{\mathsf{prE},\mathcal{D}}(\lambda)$ as

$$\mathsf{Adv}^{\mathsf{PRCtG}}_{\mathsf{prE},\mathcal{D}}(\lambda) := \left|\Pr\left[\mathsf{PRCtG}^0_{\mathsf{prE},\mathcal{D}}(\lambda) = 1\right] - \Pr\left[\mathsf{PRCtG}^1_{\mathsf{prE},\mathcal{D}}(\lambda) = 1\right]\right|.$$

Definition 4. *A triplet of algorithms* $\mathsf{prE} = (\mathsf{prE.Gen}, \mathsf{prE.Enc}, \mathsf{prE.Dec})$ *is a secret key encryption scheme with pseudorandom ciphertexts if for every* PPT *adversary* $\mathcal{D}$ *it holds that*

$$\mathsf{Adv}^{\mathsf{PRCtG}}_{\mathsf{prE},\mathcal{D}}(\lambda) \leq \mathsf{negl}(\lambda).$$

Observe that pseudorandomness of ciphertexts implies IND-CPA security.

2.2 Public Key Encryption

Definition 5 (PKE). *A* public-key encryption (PKE) *scheme* E*, with message space* $\mathcal{M}$ *and ciphertext space* $\mathcal{C}$*, consists of the following probabilistic algorithms:*

$\mathsf{E.Gen}(1^\lambda)$**:** *Given an unary encoded security parameter* λ *as input, it outputs a public key* pk *and a secret key* sk*.*

$\mathsf{E.Enc}(\mathsf{pk}, m)$**:** *Given a public key* pk *and a message* $m \in \mathcal{M}$ *as input, it outputs a ciphertext* $c \in \mathcal{C}$*.*

$\mathsf{E.Dec}(\mathsf{sk}, c)$**:** *Given a secret key* sk *and a ciphertext* $c \in \mathcal{C}$ *as input, it outputs a message* $m \in \mathcal{M}$ *or* $\perp$ *(indicating a failure).*

We use $\mathcal{R}$ *to denote the set of all possible random coins for* $\mathsf{E.Enc}$*. We require perfect correctness, that is, for every* $m \in \mathcal{M}$*, all* $(\mathsf{pk}, \mathsf{sk}) \leftarrow^{\$} \mathsf{E.Gen}(1^\lambda)$*, and all* $c \leftarrow^{\$} \mathsf{E.Enc}(\mathsf{pk}, m)$ *we have* $\mathsf{E.Dec}(\mathsf{sk}, c) = m$*. We also require that, given the public key, one can efficiently check membership in* $\mathcal{C}$*. Note that, in general,* $\mathcal{C}$ *can be larger than the range of algorithm* $\mathsf{E.Enc}(\mathsf{pk}, \cdot)$*.*

Definition 6 (IND-RCCA Secure Encryption). *A PKE scheme* $\mathsf{E} = (\mathsf{E.Gen}, \mathsf{E.Enc}, \mathsf{E.Dec})$ *is* IND-RCCA secure *(indistinguishable under replayable chosen-ciphertext attacks) if for all probabilistic polynomial-time (PPT) adversaries* $\mathcal{A}$*, it holds that:*

$$\mathsf{Adv}^{\mathsf{IND\text{-}RCCA}}_{\mathsf{E},\mathcal{A}}(\lambda) := \left| \Pr[\mathsf{IND\text{-}RCCA}^{\mathcal{A}}_{\mathsf{E}}(1^\lambda) = 1] - \frac{1}{2} \right| \leq \mathsf{negl}(\lambda)$$

where the IND-RCCA *security game is defined in Fig. 2.*

$\mathsf{IND\text{-}RCCA}^{\mathcal{A}}_{\mathsf{E}}(1^\lambda)$	$\mathsf{E.Dec}^{\diamond}(\mathsf{sk}, m_0, m_1, c)$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow^{\$} \mathsf{E.Gen}(1^\lambda)$	$m = \mathsf{E.Dec}(\mathsf{sk}, c)$
$(m_0, m_1) \leftarrow^{\$} \mathcal{A}^{\mathsf{E.Dec}(\mathsf{sk},\cdot)}(\mathsf{pk})$	**if** $m \in \{m_0, m_1\}$
$b \leftarrow^{\$} \{0,1\}$	**return** $\diamond$
$c^* \leftarrow^{\$} \mathsf{E.Enc}(\mathsf{pk}, m_b)$	**else**
$b' \leftarrow^{\$} \mathcal{A}^{\mathsf{E.Dec}^{\diamond}(\mathsf{sk},m_0,m_1,\cdot)}(c^*)$	**return** m
return $b = b'$	

Fig. 2. IND-RCCA security game.

Definition 7 (Re-randomizability). *A* re-randomizable *PKE is a PKE with the following additional probabilistic algorithm:*

$\mathsf{Rerand}(\mathsf{pk}, c)$**:** *Given a public key* pk *and a ciphertext* $c \in \mathcal{C}$ *as input, it outputs a ciphertext* $c' \in \mathcal{C}$*.*

For correctness we additionally require that for every $m \in \mathcal{M}$*, all* $(\mathsf{pk}, \mathsf{sk}) \leftarrow^{\$} \mathsf{E.Gen}(1^\lambda)$*, and all* $c \leftarrow^{\$} \mathsf{E.Enc}(\mathsf{pk}, m)$*, we have* $\mathsf{E.Dec}(\mathsf{sk}, \mathsf{Rerand}(\mathsf{pk}, c)) = m$*.*

Definition 8 (RAND-CCA1). *A re-randomizable PKE scheme* E *is* RAND-CCA1 secure *if for all PPT adversaries* $\mathcal{A}$ *the following holds:*

$$\mathsf{Adv}^{\mathsf{RAND\text{-}CCA1}}_{\mathsf{E},\mathcal{A}}(\lambda) := \left| \Pr[\mathsf{RAND\text{-}CCA1}_{\mathsf{E},\mathcal{A}}(1^\lambda) = 1] - \frac{1}{2} \right| \leq \mathsf{negl}(\lambda)$$

where the RAND-CCA1 *security game is defined in Fig. 3.*

The definition of RAND-CPA is analogous to the previous one, with the difference that no decryption queries are allowed at all in the RAND-CPA game.

$\mathsf{RAND\text{-}CCA1}_{\mathsf{E},\mathcal{A}}(1^\lambda)$

1 : $(\mathsf{pk}, \mathsf{sk}) \leftarrow^{\$} \mathsf{E.Gen}(1^\lambda)$
2 : $(\widetilde{c}) \leftarrow^{\$} \mathcal{A}^{\mathsf{E.Dec}(\mathsf{sk},\cdot)}(\mathsf{pk})$
3 : $\widetilde{m} = \mathsf{E.Dec}(\mathsf{sk}, \widetilde{c})$
4 : **if** $\widetilde{m} == \perp$ **then** $c^* = \perp$
5 : **else**
6 : $\quad b \leftarrow^{\$} \{0,1\}$
7 : $\quad$ **if** $b = 1$ **then** $c^* \leftarrow^{\$} \mathsf{Rerand}(\mathsf{pk}, \widetilde{c})$
8 : $\quad$ **if** $b = 0$ **then** $c^* \leftarrow^{\$} \mathsf{E.Enc}(\mathsf{pk}, \widetilde{m})$
9 : $b' \leftarrow^{\$} \mathcal{A}(c^*)$
10 : **return** $b = b'$

Fig. 3. RAND-CCA1 security game

Definition 9 (Perfect re-randomizability). *A re-randomizable PKE scheme* E *is* perfectly re-randomizable *if for all* $\lambda \in \mathbb{N}$*, for all* $(\mathsf{pk}, \mathsf{sk}) \leftarrow^{\$} \mathsf{E.Gen}(1^\lambda)$*, for all (possibly malicious)* $\widetilde{c} \in \mathcal{C}$ *such that* $\mathsf{E.Dec}(\mathsf{sk}, \widetilde{c}) = \widetilde{m} \neq \perp$*, we have:*

$$\{\mathsf{pk}, \mathsf{sk}, \mathsf{Rerand}(\mathsf{pk}, \widetilde{c})\} \equiv \{\mathsf{pk}, \mathsf{sk}, \mathsf{E.Enc}(\mathsf{pk}, \widetilde{m})\}\,.$$

Clearly, a perfectly re-randomizable PKE scheme is also RAND-CCA1 secure, as knowledge of the secret key implies indistinguishability of fresh ciphertexts and re-randomized ciphertexts even given a decryption oracle.

We also recall in App. A.1 the notion of IND-CCA2 and in App. A.2 non-malleability under chosen-plaintext attacks of [31].

2.3 Deterministic PKE

Definition 10 (Deterministic Public-Key Encryption [6]). *An ℓ-bit* deterministic public-key encryption scheme $\mathsf{E} = (\mathsf{E.Gen}, \mathsf{E.Enc}, \mathsf{E.Dec})$ *is defined as follows.*

- $\mathsf{E.Gen}(1^\lambda)$*: On input the security parameter λ, outputs a key pair* $(\mathsf{pk}, \mathsf{sk})$.
- $\mathsf{E.Enc}(\mathsf{pk}, m)$*: On input a public key* pk *and message m from the message space $\mathcal{M}$, outputs a ciphertext $c \in \mathcal{C}$. The algorithm is* deterministic.
- $\mathsf{E.Dec}(\mathsf{sk}, c)$*: On input a secret key* sk *and ciphertext $c \in \mathcal{C}$, outputs a message $m \in \mathcal{M}$ or $\perp$.*

Definition 11 (Correctness). *Correctness requires that* $\forall(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{E.Gen}(1^\lambda)$ *and for all* $\forall m \in \mathcal{M}$ *it holds that* $\mathsf{E.Dec}(\mathsf{sk}, \mathsf{E.Enc}(\mathsf{pk}, m)) = m$.

We use the definition of PRIV1-IND security from [6, Definition 2], for simplicity we call this property PRIV security.

Definition 12 (PRIV Security). *Let* $\mathsf{E} = (\mathsf{E.Gen}, \mathsf{E.Enc}, \mathsf{E.Dec})$ *be an ℓ-bit deterministic public-key encryption scheme.* E *is PRIV secure for (t, ℓ)-sources if for any (t, ℓ)-sources M_0 and M_1 and all PPT adversaries $\mathcal{A}$, the PRIV-advantage*

$$\mathsf{Adv}^{\mathsf{priv}}_{\mathsf{E},\mathcal{A},M_0,M_1}(\lambda) := \big|\Pr[\mathsf{PRIV}^0_{\mathcal{A}}(\lambda, M_0, M_1) = 1] - \Pr[\mathsf{PRIV}^1_{\mathcal{A}}(\lambda, M_0, M_1) = 1]\big| \leq \mathsf{negl}(\lambda)$$

where the PRIV *experiment for an adversary $\mathcal{A}$ is defined in Fig. 4.*

$\mathsf{PRIV}^b_{\mathcal{A}}(\lambda, M_0, M_1)$

1 : $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{E.Gen}(1^\lambda)$
2 : $m_b \leftarrow^{\$} M_b$
3 : $c = \mathsf{E.Enc}(pk, m_b)$
4 : $b' \leftarrow \mathcal{A}^{\mathsf{E.Dec}(\mathsf{sk},\cdot)}(\mathsf{pk}, c)$
5 : **return** $b = b'$

Fig. 4. PRIV security game.

2.4 Anamorphic Encryption

The notion of (receiver) anamorphic encryption was first introduced in [32] to model private communication in the presence of a powerful adversary who controls the PKE scheme in use and knows each user's secret key, e.g., a dictator. However, in this paper, we use a more general definition proposed in [10] which

contains [32] as a special case. To achieve the above seemingly impossible goal, the receiver is allowed to generate its own public and secret key $\mathsf{apk}, \mathsf{ask}$ in *anamorphic mode*, exchange secretly with the sender a *double key* dk, and locally storing a *trapdoor key* tk to decrypt anamorphic messages from the sender. Syntax is specified in the following definition.

Definition 13 (Anamorphic Triplet). *Formally, an anamorphic triplet* $\mathsf{AT} = (\mathsf{AT.Gen}, \mathsf{AT.Enc}, \mathsf{AT.Dec})$ *is a triplet of efficient algorithms such that*

- $\mathsf{AT.Gen}(\lambda) \xrightarrow{\$} (\mathsf{apk}, \mathsf{ask}, \mathsf{dk}, \mathsf{tk})$ *with* $\mathsf{apk}, \mathsf{ask}$ *being the anamorphic public and secret keys while* dk, tk *are the double and (a possibly empty) trapdoor key.*
- $\mathsf{AT.Enc}(\mathsf{apk}, \mathsf{dk}, m, \hat{m}) \xrightarrow{\$} c$*, with* $m \in \mathcal{M}$ *and* $\hat{m} \in \widehat{\mathcal{M}}$ *being respectively the standard and anamorphic messages in* c*.*
- $\mathsf{AT.Dec}(\mathsf{ask}, \mathsf{tk}, c) = \hat{m}/\perp$*, with* $\hat{m}$ *being the anamorphic message in* c*.*

In the definition above we do not explicitly provide $\mathsf{apk}, \mathsf{dk}$ as part of $\mathsf{AT.Dec}$ input, as we implicitly assume them to be contained in ask and tk respectively.

Definition 14 (Anamorphic Encryption). *A PKE* $\mathsf{E} = (\mathsf{E.Gen}, \mathsf{E.Enc}, \mathsf{E.Dec})$ *is an Anamorphic Encryption scheme if it is* IND-CPA *secure and there exists an anamorphic triplet* $\mathsf{AT} = (\mathsf{AT.Gen}, \mathsf{AT.Enc}, \mathsf{AT.Dec})$ *such that any* PPT *adversary* $\mathcal{A}$ *has negligible advantage, defined as*

$$\mathsf{Adv}^{\mathsf{Anam}}_{\mathcal{A},\mathsf{E},\mathsf{AT}}(\lambda) \;:=\; \left|\Pr\left[\mathsf{RealG}_{\mathsf{E}}(\lambda, \mathcal{A}) = 1\right] - \Pr\left[\mathsf{AnamorphicG}_{\mathsf{AT}}(\lambda, \mathcal{A}) = 1\right]\right|$$

where $\mathsf{RealG}_{\mathsf{E}}$ *and* $\mathsf{AnamorphicG}_{\mathsf{AT}}$ *are described in Fig. 5.*

$\mathsf{RealG}_{\mathsf{E}}(\lambda, \mathcal{A})$

1 : $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\$} \mathsf{E.Gen}(\lambda)$
2 : **return** $\mathcal{A}^{\mathcal{O}_{\mathsf{real}}}(\mathsf{pk}, \mathsf{sk})$

$\mathcal{O}_{\mathsf{real}}(m, \hat{m})$

1 : Sample a random r
2 : **return** $\mathsf{E.Enc}(\mathsf{pk}, m; r)$

$\mathsf{AnamorphicG}_{\mathsf{AT}}(\lambda, \mathcal{A})$

1 : $(\mathsf{apk}, \mathsf{ask}, \mathsf{dk}, \mathsf{tk}) \xleftarrow{\$} \mathsf{AT.Gen}(\lambda)$
2 : **return** $\mathcal{A}^{\mathcal{O}_{\mathsf{anam}}}(\mathsf{apk}, \mathsf{ask})$

$\mathcal{O}_{\mathsf{anam}}(m, \hat{m})$

1 : Sample a random r
2 : **return** $\mathsf{AT.Enc}(\mathsf{apk}, \mathsf{dk}, m, \hat{m}; r)$

Fig. 5. Anamorphic Encryption security game.

If in the above definition $\mathsf{dk} = \varepsilon$ then the scheme is said to be *Public Key Anamorphic*.

A desirable property for Anamorphic schemes is Robustness, introduced in [2]. Informally, this notion requires that it should be difficult to find a message m that, when encrypted normally and then *anamorphically* decrypted (i.e. using $\mathsf{AT.Dec}$) results in some $\hat{m} \neq \perp$. We refer to Sec. A.3 for a formal definition.

3 Re-randomization Resistant Anamorphic Encryption

Let E be a PKE scheme equipped with Anamorphic Triplet $\mathsf{AT} = (\mathsf{AT.Gen}, \mathsf{AT.Enc}, \mathsf{AT.Dec})$. The re-randomization resistance game, for a PPT adversary $\mathcal{A}$, is defined in Fig. 6.

$\mathsf{RerandG}_{\mathsf{E},\mathsf{AT}}(\lambda, \mathcal{A})$

$(\mathsf{apk}, \mathsf{ask}, \mathsf{dk}, \mathsf{tk}) \leftarrow^{\$} \mathsf{AT.Gen}(\lambda)$
$(m_0, m_1, \hat{m}) \leftarrow^{\$} \mathcal{A}(\mathsf{apk})$
$b \leftarrow^{\$} \{0, 1\}$
$c \leftarrow^{\$} \mathsf{AT.Enc}(\mathsf{apk}, \mathsf{dk}, m_b, \hat{m})$
$c' \leftarrow^{\$} \mathcal{A}(c)$
if $m_b == \mathsf{E.Dec}(\mathsf{ask}, c') \wedge \hat{m} \neq \mathsf{AT.Dec}(\mathsf{ask}, \mathsf{tk}, c')$ **then**
  return 1
return 0

Fig. 6. Re-randomization resistant AE game.

Given $\mathsf{RerandG}_{\mathsf{E},\mathsf{AT}}(\lambda, \mathcal{A})$ in Fig. 6, we define the advantage of $\mathcal{A}$ against the re-randomization resistance property as

$$\mathsf{Adv}^{\mathsf{rerand}}_{\mathcal{A},\mathsf{E},\mathsf{AT}}(\lambda) := \Pr\left[\mathsf{RerandG}_{\mathsf{E},\mathsf{AT}}(\lambda, \mathcal{A}) = 1\right].$$

Definition 15 (Re-randomization resistant AE). *An Anamorphic Encryption* E *equipped with an anamorphic triplet* AT *is said to be re-randomization resistant if for every* PPT *adversary* $\mathcal{A}$ *it holds that*

$$\mathsf{Adv}^{\mathsf{rerand}}_{\mathcal{A},\mathsf{E},\mathsf{AT}}(\lambda) \leq \frac{1}{2} + \mathsf{negl}(\lambda).$$

Remark 1. We define the property of re-randomization resistance by empowering the adversary to choose a pair of regular messages along with an anamorphic one, even though this deviates from the real-world router scenario described earlier. However, we emphasize that this stronger property captures our objective: it forces the adversary to tamper with the ciphertext by altering only the anamorphic message while leaving the regular one intact. Introducing uncertainty regarding which regular message has been encrypted it is necessary to rule out trivial attacks that apply to public-key anamorphic schemes ([33]), where an adversary could simply re-encrypt the regular message with a different anamorphic one without requiring dk. Simultaneously, this rules out attacks where the adversary encrypts the regular message using $\mathsf{E.Enc}$ (in the case of robust schemes [Sec. A.3]), which would otherwise yield $\perp \notin \widehat{\mathcal{M}}$ upon anamorphic decryption.

3.1 Preliminary results on AE

We want to point out that an Anamorphic Encryption scheme, when used in anamorphic mode, inherits the security properties of the underlying PKE. We prove the above claim for IND-CCA2 security. First of all, we define a game that models the IND-CCA2 requirement when anamorphic encryption algorithm is used to produce the challenge ciphertext in Def. 16. Then we will prove that the view of an adversary playing this game is indistinguishable from the view of an adversary playing the regular IND-CCA2 game in Thm. 1.
We will refer to the analogous property but for IND-CPA encryption as anam-CPA. An analogous of Thm. 1 can be proven in this case.

Definition 16 (Anamorphic CCA2 Secure Encryption). *An anamorphic encryption scheme* $\mathsf{E} = (\mathsf{E.Gen}, \mathsf{E.Enc}, \mathsf{E.Dec})$*, equipped with anamorphic triplet* $\mathsf{AT} = (\mathsf{AT.Gen}, \mathsf{AT.Enc}, \mathsf{AT.Dec})$ *is* anam-CCA2 secure *(indistinguishable under chosen-ciphertext attacks in anamorphic mode) if for every probability distribution* $\widehat{D}$ *with high min-entropy over* $\widehat{\mathcal{M}}$*, for all* PPT *adversaries* $\mathcal{A}$*, it holds that:*

$$\mathsf{Adv}^{\mathsf{anam\text{-}CCA2}}_{\mathsf{E},\mathsf{AT},\mathcal{A}}(\lambda) := \left| \Pr[\mathsf{anam\text{-}CCA2}^{\mathcal{A}}_{\mathsf{E},\mathsf{AT}}(1^\lambda) = 1] - \frac{1}{2} \right| \leq \mathsf{negl}(\lambda)$$

where the anam-CCA2 *game is defined in Fig. 7.*

$\mathsf{anam\text{-}CCA2}^{\mathcal{A}}_{\mathsf{E},\mathsf{AT}}(1^\lambda)$

1 : $(\mathsf{apk}, \mathsf{ask}, \mathsf{dk}, \mathsf{tk}) \leftarrow^{\$} \mathsf{AT.Gen}(1^\lambda)$
2 : $(m_0, m_1) \leftarrow^{\$} \mathcal{A}^{\mathsf{E.Dec}(\mathsf{ask},\cdot)}(\mathsf{apk})$
3 : $b \leftarrow^{\$} \{0,1\}$
4 : $\hat{m} \leftarrow^{\$} \widehat{D}(\widehat{\mathcal{M}})$
5 : $c^* \leftarrow^{\$} \mathsf{AT.Enc}(\mathsf{apk}, m_b, \hat{m})$
6 : $b' \leftarrow^{\$} \mathcal{A}^{\mathsf{E.Dec}^*(\mathsf{ask},\cdot)}(c^*)$
7 : **return** $b' = b$

Fig. 7. anam-CCA2 security game. $\mathsf{E.Dec}^*(\mathsf{ask},\cdot)$ behaves as $\mathsf{E.Dec}(\mathsf{ask},\cdot)$ with the exception that it refuses to decrypt the challenge ciphertext c^*.

With the following Theorem we show that the IND-CCA2 security of E is inherited by AT.

Theorem 1. *Assume* $\mathsf{E} = (\mathsf{E.Gen}, \mathsf{E.Enc}, \mathsf{E.Dec})$ *equipped with* $\mathsf{AT} = (\mathsf{AT.Gen}, \mathsf{AT.Enc}, \mathsf{AT.Dec})$ *is an Anamorphic Encryption scheme. If* E *is* IND-CCA2 *secure, then it is also* anam-CCA2 *secure.*

Proof. To prove Thm. 1 let us assume that there exists a distinguisher $\mathcal{D}$ that distinguishes between the regular IND-CCA2 game and anam-CCA2. We construct a distinguisher $\mathcal{A}$ against the anamorphism of E using the distinguisher $\mathcal{D}$. The pseudocode of $\mathcal{A}$ is given in Fig. 8.

$\mathcal{A}^{\mathcal{O}}(\mathsf{pk}, \mathsf{sk})$

1 : $\mathsf{Dec}(\cdot) := \mathsf{E.Dec}(\mathsf{sk}, \cdot)$
2 : $(m_0, m_1) \leftarrow^{\$} \mathcal{D}^{\mathsf{Dec}(\cdot)}(\mathsf{pk})$
3 : $b \leftarrow^{\$} \{0, 1\}$
4 : $\hat{m} \leftarrow^{\$} \widehat{D}(\widehat{\mathcal{M}})$
5 : $c^* \leftarrow^{\$} \mathcal{O}(m_b, \hat{m})$
6 : **return** $\mathcal{D}^{\mathsf{Dec}^*(\cdot)}(c^*)$

Fig. 8. $\mathcal{A}$ reducing a distinguisher $\mathcal{D}$ for IND-CCA2, anam-CCA2 to the anamorphism of E. $\mathsf{Dec}^*(\cdot)$ behaves as $\mathsf{Dec}(\cdot)$ with the exception that it refuses to decrypt the challenge ciphertext c^*.

If $\mathcal{A}$ is playing in the anamorphic game, then the keypair $(\mathsf{pk}, \mathsf{sk})$ is generated by the anamorphic key generation algorithm AT.Gen. Additionally, the challenge ciphertext c^* is computed through the anamorphic encryption algorithm AT.Enc. It follows that the view of $\mathcal{D}$ is exactly the same as in anam-CCA2. In case $\mathcal{A}$ is playing the regular game, then the keypair $(\mathsf{pk}, \mathsf{sk})$ is generated by the regular key generation algorithm E.Gen and the challenge ciphertext is computed through the regular encryption algorithm E.Enc. It holds that the view of $\mathcal{D}$ is exactly the same as in IND-CCA2. Thus, if E equipped with AT is an anamorphic encryption scheme and E is IND-CCA2 secure, then it is also anam-CCA2 secure. □

Similarly we can define non-malleability in anamorphic mode.

Definition 17 (Anamorphic Non-Malleable Encryption). *An anamorphic encryption scheme* $\mathsf{E} = (\mathsf{E.Gen}, \mathsf{E.Enc}, \mathsf{E.Dec})$*, equipped with anamorphic triplet* $\mathsf{AT} = (\mathsf{AT.Gen}, \mathsf{AT.Enc}, \mathsf{AT.Dec})$ *is* anam-NM-CPA secure *(non-malleable under chosen-plaintext attacks in anamorphic mode) if for* $\ell \in \mathbb{N}$*, for every probability distribution* $\widehat{D}$ *with high min-entropy over* $\widehat{\mathcal{M}}$*, and for all* PPT *adversaries* $\mathcal{A}$*, it holds that:*

$$\mathsf{Adv}^{\mathsf{anam\text{-}NM\text{-}CPA}}_{\mathsf{E},\mathsf{AT},\mathcal{A},\ell}(\lambda) := \Big|\Pr[\mathsf{anam\text{-}NM\text{-}CPA}^{\mathcal{A}}_{\mathsf{E},\mathsf{AT},\ell}(1^\lambda, 0) = 1] - \Pr[\mathsf{anam\text{-}NM\text{-}CPA}^{\mathcal{A}}_{\mathsf{E},\mathsf{AT},\ell}(1^\lambda, 1) = 1]\Big| \leq \mathsf{negl}(\lambda)$$

where the anam-NM-CPA *game is defined in Fig. 9.*

$\mathsf{anam\text{-}NM\text{-}CPA}^{\mathcal{A}}_{\mathsf{E},\mathsf{AT},\ell}(1^\lambda, b)$

$(\mathsf{apk}, \mathsf{ask}, \mathsf{dk}, \mathsf{tk}) \leftarrow^{\$} \mathsf{AT.Gen}(1^\lambda)$
$(m_0, m_1) \leftarrow^{\$} \mathcal{A}(\mathsf{apk})$
$\hat{m} \leftarrow^{\$} \widehat{D}(\widehat{\mathcal{M}})$
$c^* \leftarrow^{\$} \mathsf{AT.Enc}(\mathsf{apk}, m_b, \hat{m})$
$(c_1, \ldots, c_\ell) \leftarrow^{\$} \mathcal{A}(c^*)$
for $i \in \{1, \ldots, \ell\}$
  if $c_i == c^*$ **then**
    $d_i = \perp$
  else
    $d_i = \mathsf{E.Dec}(\mathsf{ask}, c_i)$
return $\mathcal{A}(d_1, \ldots, d_\ell)$

Fig. 9. anam-NM-CPA security game.

We can state a Theorem similar to Thm. 1 for the case of non-malleability. The notion of NM-CPA can be found in Sec. A.2. The proof is essentially the same and for this reason we omit it.

Theorem 2. *Assume* $\mathsf{E} = (\mathsf{E.Gen}, \mathsf{E.Enc}, \mathsf{E.Dec})$ *equipped with* $\mathsf{AT} = (\mathsf{AT.Gen}, \mathsf{AT.Enc}, \mathsf{AT.Dec})$ *is an Anamorphic Encryption scheme. If* E *is* NM-CPA *secure, then it is also* anam-NM-CPA *secure.*

It is easy to observe that, as for the regular definitions, anam-CCA2 $\implies$ anam-NM-CPA.

3.2 Generic Construction of Re-randomization Resistant AE

Let $\mathsf{E}_1 = (\mathsf{E}_1.\mathsf{Gen}, \mathsf{E}_1.\mathsf{Enc}, \mathsf{E}_1.\mathsf{Dec})$ be a NM-CPA secure public-key encryption scheme that is also anamorphic encryption scheme with an anamorphic triplet $\mathsf{AT}_1 = (\mathsf{AT}_1.\mathsf{Gen}, \mathsf{AT}_1.\mathsf{Enc}, \mathsf{AT}_1.\mathsf{Dec})$. Let $\mathsf{E}_2 = (\mathsf{E}_2.\mathsf{Gen}, \mathsf{E}_2.\mathsf{Enc}, \mathsf{E}_2.\mathsf{Dec})$ be a IND-CPA secure re-randomizable public-key encryption scheme. Assume that the ciphertext space of E_1 is $\mathcal{C}$, and that the message space of E_2 is the same set $\mathcal{C}$.

Consider the scheme $\mathsf{E} = (\mathsf{E.Gen}, \mathsf{E.Enc}, \mathsf{E.Dec})$ in Fig. 10.

Anamorphic construction. The anamorphic triplet $\mathsf{AT} = (\mathsf{AT.Gen}, \mathsf{AT.Enc}, \mathsf{AT.Dec})$ is specified in Fig. 11.

Re-randomization resistance. In the following theorem we show that the above scheme when equipped with the Anamorphic Triplet in Fig. 11 is a Re-randomization Resistant Anamorphic Encryption.

Theorem 3. *Let* E_2 *be an IND-CPA re-randomizable public-key encryption scheme with message space* $\mathcal{C}$ *and let* E_1 *be a* NM-CPA *public key anamorphic encryption*

$\mathsf{E.Gen}(\lambda)$

1 : $(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow^{\$} \mathsf{E}_1.\mathsf{Gen}(\lambda)$
2 : $(\mathsf{pk}_2, \mathsf{sk}_2) \leftarrow^{\$} \mathsf{E}_2.\mathsf{Gen}(\lambda)$
3 : $\mathsf{pk} = (\mathsf{pk}_1, \mathsf{pk}_2)$
4 : $\mathsf{sk} = (\mathsf{sk}_1, \mathsf{sk}_2)$
5 : **return** $(\mathsf{pk}, \mathsf{sk})$

$\mathsf{E.Enc}(\mathsf{pk}, m)$

1 : $c_1 \leftarrow^{\$} \mathsf{E}_1.\mathsf{Enc}(\mathsf{pk}_1, m)$
2 : $c_2 \leftarrow^{\$} \mathsf{E}_2.\mathsf{Enc}(\mathsf{pk}_2, c_1)$
3 : $c = c_2$
4 : **return** c

$\mathsf{E.Dec}(\mathsf{sk}, c)$

1 : $c_1 = \mathsf{E}_2.\mathsf{Dec}(\mathsf{sk}_2, c)$
2 : $m = \mathsf{E}_1.\mathsf{Dec}(\mathsf{sk}_1, c_1)$
3 : **return** m

Fig. 10. Generic Re-randomizable Encryption Scheme.

scheme with ciphertext space $\mathcal{C}$ *equipped with anamorphic triplet* $(\mathsf{AT}_1.\mathsf{Gen}, \mathsf{AT}_1.\mathsf{Enc}, \mathsf{AT}_1.\mathsf{Dec})$*, then the scheme* E *reported in Fig. 10 with anamorphic triplet* AT *reported in Fig. 11 is a re-randomization-resistant re-randomizable anamorphic encryption scheme (Def. 15).*

Proof. We prove the Thm. 3 through the following lemmas. We first show that E is IND-CPA secure, then we show that E equipped with AT is an anamorphic encryption scheme and eventually we prove its re-randomization resistance.

Lemma 1. *The scheme* E *in Fig. 10 is* IND-CPA *secure.*

Proof. Let us assume that there exists an adversary $\mathcal{A}$ that breaks the IND-CPA of E with overwhelming probability, we show an adversary $\mathcal{B}$ in Fig. 12 that breaks the IND-CPA of E_1 with the same probability. Note that the NM-CPA security of E_1 implies its IND-CPA security.

$\mathcal{B}$ upon receiving a public key pk_1 for E_1 produces the keypair for the external scheme E_2. This allows $\mathcal{B}$ to perfectly simulate the public key for the IND-CPA game of E. $\mathcal{B}$ encrypts with the external PKE the messages chosen by $\mathcal{A}$ before forwarding them to IND-CPA challenge oracle $\mathcal{O}$ for E_1. This perfectly simulates the challenge encryption oracle of E for $\mathcal{A}$. When $\mathcal{B}$ receives the challenge ciphertext forwards it to $\mathcal{A}$ and returns the same output as $\mathcal{A}$. Since $\mathcal{A}$ guesses the bit b for the IND-CPA game regarding E with overwhelming probability, the same holds for $\mathcal{B}$, reaching a contradiction. □

Lemma 2. *The scheme* E *in Fig. 10 with anamorphic triplet* AT *in Fig. 11 is an anamorphic encryption scheme.*

Proof. Let us assume that there exists an adversary $\mathcal{A}$ that breaks the anamorphism of E, AT with overwhelming probability, i.e., $\mathcal{A}$ distinguishes $\mathsf{RealG}_{\mathsf{E}}$ from $\mathsf{AnamorphicG}_{\mathsf{AT}}$ with overwhelming probability. We show an adversary $\mathcal{B}$ in Fig. 13 that breaks the anamorphism of $\mathsf{E}_1, \mathsf{AT}_1$ with the same probability.

$\mathsf{AT.Gen}(\lambda)$

1 : $(\mathsf{apk}_1, \mathsf{ask}_1, \mathsf{dk}_1, \mathsf{tk}_1) \leftarrow^{\$} \mathsf{AT}_1.\mathsf{Gen}(\lambda)$
2 : $(\mathsf{pk}_2, \mathsf{sk}_2) \leftarrow^{\$} \mathsf{E}_2.\mathsf{Gen}(\lambda)$
3 : $\mathsf{apk} = (\mathsf{apk}_1, \mathsf{pk}_2)$
4 : $\mathsf{ask} = (\mathsf{ask}_1, \mathsf{sk}_2)$
5 : $\mathsf{tk} = \mathsf{tk}_1$
6 : $\mathsf{dk} = \mathsf{dk}_1$
7 : **return** $(\mathsf{apk}, \mathsf{ask}, \mathsf{dk}, \mathsf{tk})$

$\mathsf{AT.Enc}(\mathsf{apk}, \mathsf{dk}, m, \hat{m})$

1 : Parse $\mathsf{apk} = (\mathsf{apk}_1, \mathsf{pk}_2)$
2 : $c_1 \leftarrow^{\$} \mathsf{AT}_1.\mathsf{Enc}(\mathsf{apk}_1, \mathsf{dk}, m, \hat{m})$
3 : $c \leftarrow^{\$} \mathsf{E}_2.\mathsf{Enc}(\mathsf{pk}_2, c_1)$
4 : **return** c

$\mathsf{AT.Dec}(\mathsf{ask}, \mathsf{tk}, c)$

1 : Parse $\mathsf{ask} = (\mathsf{ask}_1, \mathsf{sk}_2)$
2 : $c_1 = \mathsf{E}_2.\mathsf{Dec}(\mathsf{sk}_2, c)$
3 : $\hat{m} = \mathsf{AT}_1.\mathsf{Dec}(\mathsf{ask}_1, \mathsf{tk}, c_1)$
4 : **return** $\hat{m}$

Fig. 11. Anamorphic Triplet AT for the Generic Construction.

$\mathcal{B}^{\mathcal{O}}(\mathsf{pk}_1)$

1 : $(\mathsf{pk}_2, \mathsf{sk}_2) \leftarrow^{\$} \mathsf{E}_2.\mathsf{Gen}(\lambda)$
2 : $\mathsf{pk} = (\mathsf{pk}_1, \mathsf{pk}_2)$
3 : $(m_0, m_1) \leftarrow^{\$} \mathcal{A}(\mathsf{pk})$
4 : $c_0 \leftarrow^{\$} \mathsf{E}_2.\mathsf{Enc}(\mathsf{pk}_2, m_0)$
5 : $c_1 \leftarrow^{\$} \mathsf{E}_2.\mathsf{Enc}(\mathsf{pk}_2, m_1)$
6 : $c^* \leftarrow^{\$} \mathcal{O}(c_0, c_1)$
7 : **return** $\mathcal{A}(c^*)$

Fig. 12. $\mathcal{B}$ reducing an adversary $\mathcal{A}$ for IND-CPA of E to the IND-CPA of E_1. $\mathcal{O}$ is the challenge oracle for IND-CPA game of E_1.

If $\mathcal{B}$ is playing the game $\mathsf{AnamorphicG}_{\mathsf{AT}_1}$ this means that $\mathsf{pk}_1, \mathsf{sk}_1$ are computed through $\mathsf{AT}_1.\mathsf{Gen}$ and that c is computed as $\mathsf{AT.Enc}(\mathsf{pk}_1, \mathsf{dk}, m, \hat{m})$. If $\mathcal{B}$ is playing the game $\mathsf{RealG}_{\mathsf{E}_1}$ this means that $\mathsf{pk}_1, \mathsf{sk}_1$ are computed through $\mathsf{E}_1.\mathsf{Gen}$ and that c is computed as $\mathsf{E}_1.\mathsf{Enc}(\mathsf{pk}_1, m)$. In both cases $\mathcal{B}$ produces the outer layer keypair $(\mathsf{pk}_2, \mathsf{sk}_2)$ and encrypts the ciphertext c_1 obtained from its challenge oracle using $\mathsf{E}_2.\mathsf{Enc}(\mathsf{pk}_2, c_1)$. This perfectly simulates the $\mathsf{AnamorphicG}_{\mathsf{AT}}$ and $\mathsf{RealG}_{\mathsf{E}}$ games for $\mathcal{A}$. Given this fact, any non-negligible advantage of $\mathcal{A}$ in distinguishing $\mathsf{AnamorphicG}_{\mathsf{AT}}$ and $\mathsf{RealG}_{\mathsf{E}}$ translates directly to the same advantage for $\mathcal{B}$ in breaking E_1's anamorphic security, i.e., distinguishing $\mathsf{AnamorphicG}_{\mathsf{AT}_1}$ and $\mathsf{RealG}_{\mathsf{E}_1}$. □

Lemma 3. *The scheme* E *in Fig. 10 is a re-randomization resistant anamorphic encryption scheme (following Def. 15).*

$\mathcal{B}^{\mathcal{O}}(\mathsf{pk}_1, \mathsf{sk}_1)$

$(\mathsf{pk}_2, \mathsf{sk}_2) \leftarrow^{\$} \mathsf{E}_2.\mathsf{Gen}(\lambda)$
$\mathsf{pk} = (\mathsf{pk}_1, \mathsf{pk}_2)$
$\mathsf{sk} = (\mathsf{sk}_1, \mathsf{sk}_2)$
Run $\mathcal{A}(\mathsf{pk}, \mathsf{sk})$
Whenever $\mathcal{A}$ queries $(m, \hat{m})$:
  $c_1 \leftarrow^{\$} \mathcal{O}(m, \hat{m})$
  $c \leftarrow^{\$} \mathsf{E}_2.\mathsf{Enc}(\mathsf{pk}_2, c_1)$
  Give c to $\mathcal{A}$
return $\mathcal{A}$'s output

Fig. 13. $\mathcal{B}$ reducing an adversary $\mathcal{A}$ for anamorphism of E, AT to the anamorphism of $\mathsf{E}_1, \mathsf{AT}_1$. $\mathcal{O}$ is the anamorphic challenge oracle for $\mathsf{RealG}_{\mathsf{E}_1}$ or $\mathsf{AnamorphicG}_{\mathsf{AT}_1}$, depending on the played game.

Proof. he proof proceeds reducing an adversary $\mathcal{B}$ for the re-randomization resistance game to an adversary $\mathcal{A}$ for the anam-NM-CPA security of the underlying scheme. The pseudocode of $\mathcal{A}$ is given in Fig. 14.

$\mathcal{A}^{\mathcal{O}}(\mathsf{apk})$

$(m_0, m_1, \hat{m}) \leftarrow^{\$} \mathcal{B}(\mathsf{apk})$
$c^* \leftarrow^{\$} \mathcal{O}(m_0, m_1, \hat{m})$
$c' \leftarrow^{\$} \mathcal{B}(c^*)$
$d = \mathcal{O}(c')$
if $d == m_0$ **then**
  return 0
elseif $d == m_1$ **then**
  return 1

Fig. 14. $\mathcal{A}$ reducing an adversary $\mathcal{B}$ for rerand to the anam-NM-CPA security of E, AT, for $\ell = 1$. $\mathcal{O}$ is the challenge oracle of the anam-NM-CPA game: on input two regular messages and an anamorphic one it returns the challenge ciphertext c^*; on input a ciphertext c' it returns its decryption iff $c^* \neq c'$.

Note that the view of $\mathcal{B}$ is perfectly simulated by $\mathcal{A}$. Indeed, the keys in anam-NM-CPA are generated through AT.Gen and if $\mathcal{A}$ is playing anam-NM-CPA(0) then messages $m_0, \hat{m}$ are encrypted using AT.Enc. While if $\mathcal{A}$ is playing anam-NM-CPA(1) then messages $m_1, \hat{m}$ are encrypted using AT.Enc. Thus, $\mathcal{A}$ perfectly simulates the view of $\mathcal{B}$ for the game $\mathsf{RerandG}_{\mathsf{E},\mathsf{AT}}$. Given that $\mathcal{B}$ is an adversary that wins the $\mathsf{RerandG}_{\mathsf{E},\mathsf{AT}}$ game, it follows that the ciphertext c' is a ciphertext that

decrypts to m_b and that contains an anamorphic message $\tilde{m} \neq \hat{m}$. These two facts imply that $c' \neq c^*$. Thus, the challenger for anam-NM-CPA game will give back $d = m_b$ to $\mathcal{A}$. Now $\mathcal{A}$ can easily distinguish the two games. It holds that $\mathcal{A}$ distinguish anam-NM-CPA(0) from anam-NM-CPA(1) with the same probability of $\mathcal{B}$ winning $\mathsf{RerandG}_{\mathsf{E},\mathsf{AT}}$.
This proves that if E, AT is an anam-NM-CPA secure encryption scheme, then it is also re-randomization resistant. □

The theorem follows from the previous lemmas. □

3.3 On the Existence of anam-NM-CPA AE

In order to prove the existence of re-randomization resistant AE, in Thm. 3 we need to assume the existence of an anamorphic encryption scheme $\mathsf{E}_1, \mathsf{AT}_1$ that is NM-CPA secure. Here we discuss about the existence of such scheme.

anam-NM-CPA AE from anam-CPA AE. In [13] it is shown how to obtain a NM-CPA secure PKE E^* from an IND-CPA secure PKE E in a black-box way. This is done adding digital signature and verification steps, along with encodings of the message to be encrypted with a randomized Reed-Solomon code. The rate[8] of this construction is improved in [15] replacing the code used originally. We elaborate on the fact that if E with anamorphic triplet AT is an anamorphic encryption scheme then also E^* is an anamorphic encryption scheme. Indeed, since the construction is black-box, we can construct the anamorphic triplet AT^* for E^* simply substituting the regular algorithms of E with their anamorphic counterparts. The anamorphic triplet AT^* is made out of the same algorithms $(\mathsf{E}^*\mathsf{Gen}, \mathsf{E}^*.\mathsf{Enc})$ except for the fact that the calls to $(\mathsf{E.Gen}, \mathsf{E.Enc})$ are substituted by calls to their anamorphic versions $(\mathsf{AT.Gen}, \mathsf{AT.Enc}, \mathsf{AT.Dec})$. The only exception is the anamorphic decryption algorithm $\mathsf{AT}^*.\mathsf{Dec}$ that directly returns the output of $\mathsf{AT.Dec}$ without performing other operations. The anamorphism of $\mathsf{E}^*, \mathsf{AT}^*$ follows by a straightforward reduction from the anamorphism of E, AT. Applying Thm. 2 we obtain that $\mathsf{E}^*, \mathsf{AT}^*$ is anam-NM-CPA. Finally, we know that any IND-CPA PKE E with high min-entropy ciphertexts[9] can be turned anamorphic [12] using the rejection sampling technique from [32]. This allows us to state the following Corollary.

Corollary 1. *If* IND-CPA *public key encryption schemes with high min-entropy ciphertexts exist, then there exists Re-randomization Resistant Anamorphic Encryption.*

The high min-entropy ciphertexts is a property satisfied by most of the PKEs used in practice, concrete examples are [20, 30, 36].

[8] I.e., ciphertext length divided by plaintext length.
[9] I.e., for any $(\mathsf{pk}, \mathsf{sk})$ in the range of $\mathsf{E.Gen}$ algorithm, and for any message m in the message space it holds that $\mathrm{H}_\infty(\mathsf{E.Enc}(\mathsf{pk}, m)) = \Omega(\lambda)$ (See [12]).

anam-NM-CPA AE from anam-CCA2 AE. In the following we state a Theorem obtained combining two theorems from [19] that will be useful to prove the existence of anam-NM-CPA secure schemes.
[19, Theorem 9.5] states that if there exists any IND-CCA2 encryption scheme, then, in the Random Oracle Model, there exists a scheme that is IND-CCA2 and additionally allows to recover the randomness used to produce a ciphertext c from c itself and the secret key. This property is called the *strong randomness recoverability*. [19, Theorem 9.7] states that any strong randomness recoverable PKE can be turned anamorphic (with some additional properties). Combining the two Theorems we obtain the following Theorem.

Theorem 4 ([19], Theorems 9.5 + 9.7). *If there exists* IND-CCA2 *public key encryption, then, in the Random Oracle Model, there exists Anamorphic Encryption.*

Since in Thm. 1 we proved that the anamorphic encryption algorithm inherits the security properties of the underlying PKE, combining Thm. 4 with the fact that IND-CCA2 $\implies$ NM-CPA, Thm. 1 and Thm. 3 we obtain the following Corollary.

Corollary 2. *If* IND-CCA2 *public key encryption exists, then, in the Random Oracle model, there exist Re-randomization Resistant Anamorphic Encryption.*

Finally, we want to point out that in the literature several IND-CCA2 schemes have been proven to be Anamorphic. Some examples are the Naor-Yung transform [29, 37] in [32], the Cramer-Shoup and SPHF-based cryptosystems [16, 17] in [27], the Koppula-Waters scheme [25] and any IND-CCA2 PKE that is black-box reduced from an IND-CPA PKE in [33].

4 Deterministic Anamorphic Encryption

We also introduce a definition in which the message to be encrypted is randomly chosen by the challenger.

This definition is motivated by a scenario in robust anamorphic encryption, where each machine is connected to a server controlled by a dictator. The server contains all users' secret keys, and each message passes through it for decryption and re-encryption. In non-robust schemes, decrypting and re-encrypting a ciphertext destroys the anamorphic message except with probability proportional to $|\widehat{\mathcal{M}}|$, since encrypting a message with the standard encryption algorithm has $|\widehat{\mathcal{M}}|^{-1}$ probability to produce a ciphertext that anamorphically decrypt to the same anamorphic message. In robust schemes, the anamorphic message is destroyed with probability 1 since re-encrypting a message using the standard encryption algorithm always produces a ciphertext that the anamorphic decryption algorithm outputs $\perp$ on. Deterministic Anamorphic Encryption represents the opposite scenario, indeed, while in normal anamorphic schemes the idea is

to hide the anamorphic message in the randomness used to encrypt, in Deterministic Anamorphic Encryption the encoded anamorphic message is the regular message to be encrypted. In this scenario, the challenge message is randomly sampled by the challenger, and the dictator cannot destroy the anamorphic message without compromising the real message. Uniformly sampled messages are necessary in the context of deterministic PKE [6].

Definition 18 (Deterministic Anamorphic Triplet). *A Deterministic Anamorphic Triplet* $\mathsf{ATR} = (\mathsf{ATR.Gen}, \mathsf{ATR.Enc}, \mathsf{ATR.Dec})$ *is a triplet of efficient algorithms such that*

- $\mathsf{ATR.Gen}(\lambda) \xrightarrow{\$} (\mathsf{apk}, \mathsf{ask}, \mathsf{dk}, \mathsf{tk})$*, with* $\mathsf{apk}, \mathsf{ask}$ *being the anamorphic public and secret keys, and* dk, tk *being the double key and (possibly empty) trapdoor key, respectively.*
- $\mathsf{ATR.Enc}(\mathsf{apk}, \mathsf{dk}, \hat{m}) \xrightarrow{\$} c$*, with* $\hat{m} \in \widehat{\mathcal{M}}$ *being the anamorphic message encrypted in* c*.*
- $\mathsf{ATR.Dec}(\mathsf{ask}, \mathsf{tk}, c) = \hat{m}/\perp$*, where* $\hat{m}$ *is the anamorphic message encrypted in* c*.*

Definition 19 (Deterministic Anamorphic Encryption). *A deterministic PKE* $\mathsf{E} = (\mathsf{E.Gen}, \mathsf{E.Enc}, \mathsf{E.Dec})$ *is a Deterministic Anamorphic Encryption scheme if it is PRIV secure with message space* $\mathcal{M}$ *and there exists an anamorphic triplet* $\mathsf{ATR} = (\mathsf{ATR.Gen}, \mathsf{ATR.Enc}, \mathsf{ATR.Dec})$ *such that any* PPT *adversary* $\mathcal{A}$ *has negligible advantage, defined as*

$$\mathsf{Adv}^{\mathsf{Anam}}_{\mathcal{A},\mathsf{E},\mathsf{AT}}(\lambda) := \left|\Pr\left[\mathsf{RealRG}_{\mathsf{E}}(\lambda, \mathcal{A}) = 1\right] - \Pr\left[\mathsf{AnamorphicRG}_{\mathsf{ATR}}(\lambda, \mathcal{A}) = 1\right]\right|,$$

where $\mathsf{RealRG}_{\mathsf{E}}$ *and* $\mathsf{AnamorphicRG}_{\mathsf{ATR}}$ *are the same games reported in Fig. 5 but using the oracles described in Fig. 15.*

$\mathcal{O}_{\mathsf{real}}(\hat{m})$	$\mathcal{O}_{\mathsf{anam}}(\hat{m})$
$m \xleftarrow{\$} \mathcal{M}$	**return** $\mathsf{ATR.Enc}(\mathsf{apk}, \mathsf{dk}, \hat{m})$
return $\mathsf{E.Enc}(\mathsf{pk}, m)$	

Fig. 15. Deterministic Anamorphic Encryption security game oracles.

Instantiating deterministic anamorphic encryption. In the following we show that every scheme $\mathsf{E}_{\mathsf{det}} = (\mathsf{Gen}_{\mathsf{det}}, \mathsf{Enc}_{\mathsf{det}}, \mathsf{Dec}_{\mathsf{det}})$ that is PRIV secure it is a Deterministic Anamorphic Encryption scheme with uniform message space distribution. Notice that in our paper we consider only deterministic public-key encryption schemes where the message space $\mathcal{M}$ is taken to be $\{0,1\}^n$ for some fixed $n = \mathsf{poly}(\lambda)$, and messages are assumed to be distributed uniformly over $\mathcal{M}$.

$\mathsf{ATR.Gen}(\lambda)$

1 : $(\mathsf{pk}, \mathsf{sk}) \leftarrow^{\$} \mathsf{E.Gen}_{\mathsf{det}}(\lambda)$
2 : $k \leftarrow^{\$} \mathsf{Gen}_{\mathsf{rand}}(\lambda)$
3 : $\mathsf{apk} = \mathsf{pk}, \mathsf{ask} = \mathsf{sk}, \mathsf{dk} = k, \mathsf{tk} = k$
4 : **return** $(\mathsf{apk}, \mathsf{ask}, \mathsf{dk}, \mathsf{tk})$

$\mathsf{ATR.Enc}(\mathsf{apk}, \mathsf{dk}, \hat{m})$

1 : $c = \mathsf{E.Enc}_{\mathsf{det}}(\mathsf{apk}, \mathsf{Enc}_{\mathsf{rand}}(\mathsf{dk}, \hat{m}))$
2 : **return** c

$\mathsf{ATR.Dec}(\mathsf{ask}, \mathsf{tk}, c)$

1 : $c' = \mathsf{E.Dec}_{\mathsf{det}}(\mathsf{ask}, c)$
2 : $\hat{m} = \mathsf{Dec}_{\mathsf{rand}}(\mathsf{tk}, c')$
3 : **return** $\hat{m}$

Fig. 16. Anamorphic Triplet ATR for the Deterministic Anamorphic Encryption scheme.

Let $\mathsf{E}_{\mathsf{det}} = (\mathsf{Gen}_{\mathsf{det}}, \mathsf{Enc}_{\mathsf{det}}, \mathsf{Dec}_{\mathsf{det}})$ be a PRIV secure public key encryption scheme and $\mathsf{E}_{\mathsf{rand}} = (\mathsf{Gen}_{\mathsf{rand}}, \mathsf{Enc}_{\mathsf{rand}}, \mathsf{Dec}_{\mathsf{rand}})$ be a SKE scheme with pseudorandom ciphertext (Def. 4).

Theorem 5. *Let* $\mathsf{E}_{\mathsf{det}} = (\mathsf{Gen}_{\mathsf{det}}, \mathsf{Enc}_{\mathsf{det}}, \mathsf{Dec}_{\mathsf{det}})$ *be a PRIV secure public key encryption scheme with uniform message space* $\mathcal{M} = \{0,1\}^n$ *distribution, for a fixed* $n = \mathsf{poly}(\lambda)$ *and a SKE scheme with pseudorandom ciphertext* $\mathsf{E}_{rand} = (\mathsf{Gen}_{\mathsf{rand}}, \mathsf{Enc}_{\mathsf{rand}}, \mathsf{Dec}_{\mathsf{rand}})$*, with ciphertext space* $\mathcal{M}$*. The scheme* $\mathsf{E}_{\mathsf{det}}$ *equipped with Anamorphic Triplet* ATR *in Fig. 16 is a Deterministic Anamorphic Encryption with message space* $\mathcal{M}$*.*

Proof. PRIV security trivially follows from the hypothesis on $\mathsf{E}_{\mathsf{det}}$, then we prove the theorem showing that $\mathsf{E}_{\mathsf{det}}$ along with anamorphic triplet ATR is a Deterministic AE through the following lemma.

Lemma 4. *The scheme* $\mathsf{E}_{\mathsf{det}} = (\mathsf{Gen}_{\mathsf{det}}, \mathsf{Enc}_{\mathsf{det}}, \mathsf{Dec}_{\mathsf{det}})$ *is a Deterministic Anamorphic Encryption scheme when equipped with the anamorphic triplet* (ATR.Gen, ATR.Enc, ATR.Dec) *in Fig. 16.*

Proof. This can be proven via the following sequence of hybrids:

Hybrid $\mathcal{H}_0$**:** Equivalent to $\mathsf{AnamorphicRG}_{\mathsf{AT}}(\lambda, \mathcal{A})$.
Hybrid $\mathcal{H}_1$**:** Equivalent to $\mathcal{H}_0$ except that we replace the call to $\mathsf{Enc}_{\mathsf{rand}}(\mathsf{dk}, \hat{m})$ with a truly random string $m \leftarrow^{\$} \{0,1\}^n$.
Hybrid $\mathcal{H}_2$**:** Equivalent to $\mathsf{RealRG}_{\mathsf{AT}}(\lambda, \mathcal{A})$.

Claim. $\mathcal{H}_0$ is computationally indistinguishable from $\mathcal{H}_1$.

Proof. The only difference is that in $\mathcal{H}_0$, the message encrypted is $\mathsf{Enc}_{\mathsf{rand}}(k, \hat{m})$, while in $\mathcal{H}_1$, the message encrypted is a truly random string $m \leftarrow^{\$} \{0,1\}^n$. By assumption, $\mathsf{E}_{\mathsf{rand}} = (\mathsf{Gen}_{\mathsf{rand}}, \mathsf{Enc}_{\mathsf{rand}}, \mathsf{Dec}_{\mathsf{rand}})$ produces ciphertexts indistinguishable from random. Hence, no PPT adversary $\mathcal{A}$ can distinguish $\mathcal{H}_0$ from $\mathcal{H}_1$ with non-negligible advantage.

If there exists a PPT adversary $\mathcal{A}$ distinguishing $\mathcal{H}_0$ from $\mathcal{H}_1$ with non-negligible advantage, then we can define an adversary $\mathcal{B}$ that breaks the ciphertext pseudorandomness of $\mathsf{E}_{\mathsf{rand}}$ with at least the same advantage.

Let $\mathcal{B}$ the adversary that exploits $\mathcal{A}$ to win the pseudorandom ciphertext game against the challenger Chal.

- Chal generates k and give the oracle $\mathcal{O}$ to $\mathcal{B}$. $\mathcal{O}$, on input $\hat{m}$, returns a random string in $\{0,1\}^n$ or an encryption of $\hat{m}$ using the key k.
- $\mathcal{B}$ produces the keypair $(\mathsf{pk}, \mathsf{sk}) \leftarrow^{\$} \mathsf{E.Gen}_{\mathsf{det}}(\lambda)$
- $\mathcal{B}$ waits for anamorphic messages from $\mathcal{A}(\mathsf{pk}, \mathsf{sk})$.
- Every time that $\mathcal{A}$ sends a message $\hat{m}$ to $\mathcal{B}$, $\mathcal{B}$ redirect this message to Chal receiving back m.
  $\mathcal{B}$ computes $c = \mathsf{E.Enc}_{\mathsf{det}}(\mathsf{pk}, m)$ and sends c to $\mathcal{A}$.
- When $\mathcal{A}$ returns an output, $\mathcal{B}$ returns the same output to Chal.

Notice that this execution perfectly simulates $\mathcal{H}_0$ if Chal executes the encryption of the message and perfectly simulates $\mathcal{H}_1$ otherwise, therefore if $\mathcal{A}$ is able to distinguish $\mathcal{H}_0$ from $\mathcal{H}_1$ with non-negligible advantage $\mathcal{B}$ breaks the pseudorandom ciphertext game of $\mathsf{E}_{\mathsf{rand}}$ that is a contradiction. □

Claim. $\mathcal{H}_1$ is indistinguishable from $\mathcal{H}_2$.

Proof. The only difference is the key generation: $\mathcal{H}_1$ generates $(\mathsf{apk}, \mathsf{ask}, k, k) \leftarrow^{\$} \mathsf{ATR.Gen}(\lambda)$, while $\mathcal{H}_2$ generates $(\mathsf{pk}, \mathsf{sk}) \leftarrow^{\$} \mathsf{Gen}_{\mathsf{rand}}$. The pair $(\mathsf{apk}, \mathsf{ask})$ and $(\mathsf{pk}, \mathsf{sk})$ in the two hybrids are generated with the same algorithm, therefore are distributed identically, while the additional key k in $\mathcal{H}_1$ is never used. Also the encryption oracles are identical in both hybrids, therefore, the two hybrids are indistinguishable to any adversary. □

The lemma follows from previous claims. □

The theorem follows from the previous lemma and PRIV security of $\mathsf{E}_{\mathsf{rand}}$. □

A concrete instantiation. An example of concrete instantiation for E is given by:

- $\mathsf{E}_{\mathsf{det}} = (\mathsf{Gen}_{\mathsf{det}}, \mathsf{Enc}_{\mathsf{det}}, \mathsf{Dec}_{\mathsf{det}})$ instantiated using one of the schemes proposed in [3, 7, 40]:
  - with [3] we obtain a PRIV secure scheme in the random oracle model, assuming RSA;
  - with [7] we obtain a scheme secure in the auxiliary-input setting under the DLin assumption;
  - with [40] we obtain a scheme secure under one of the following assumptions: DDH, DLin, LWE, or QR.
- $\mathsf{E}_{\mathsf{rand}}$ instantiated as follows using AES:
  - $\mathsf{Gen}_{\mathsf{rand}}(\lambda)$: generate a secret AES key k and return k;
  - $\mathsf{Enc}_{\mathsf{rand}}(k, m)$: generate a random IV, compute $c = \mathsf{AES}(k, IV, m)$, and return (c, IV);

- $\mathsf{Dec}_{\mathsf{rand}}(k, IV, c)$: compute $m = \mathsf{AES}^{-1}(k, IV, c)$ and return m if decryption is valid, else $\perp$.

The respective anamorphic triplet is:

- $\mathsf{ATR.Gen}(\lambda)$: run $(\mathsf{pk}, \mathsf{sk}) \leftarrow^{\$} \mathsf{E.Gen}_{\mathsf{det}}(\lambda)$, $k \leftarrow^{\$} \mathsf{Gen}_{\mathsf{rand}}$, and return $(\mathsf{apk} = \mathsf{pk}, \mathsf{ask} = \mathsf{sk}, \mathsf{dk} = k, \mathsf{tk} = k)$.
- $\mathsf{ATR.Enc}(\mathsf{apk}, \mathsf{dk}, \hat{m})$: compute $c = \mathsf{E.Enc}_{\mathsf{det}}(\mathsf{apk}, IV || \mathsf{Enc}_{\mathsf{rand}}(k, \hat{m}))$ and return c.
- $\mathsf{AT.Dec}(\mathsf{ask}, \mathsf{tk}, c)$: compute $(IV || c') = \mathsf{E.Dec}_{\mathsf{det}}(\mathsf{ask}, c)$, then $\hat{m} = \mathsf{Dec}_{\mathsf{rand}}(k, IV, c')$ and return $\hat{m}$ if valid, else $\perp$.

5 Black-box Re-randomizable PKE

In this section we show that our generic solution to achieve Re-randomization Resistant AE (Sec. 3.2) reaches different desirable security properties, varying the assumptions made for its building blocks.

5.1 Two-Layer Construction

Let $\mathsf{E}_1 = (\mathsf{E.Gen}_1, \mathsf{E.Enc}_1, \mathsf{E.Dec}_1)$ be a PKE scheme with message space $\mathcal{M}_1$ and ciphertext space $\mathcal{C}_1$, and let $\mathsf{E}_2 = (\mathsf{E.Gen}_2, \mathsf{E.Enc}_2, \mathsf{E.Dec}_2, \mathsf{Rerand})$ be a re-randomizable PKE scheme with message space $\mathcal{M}_2 = \mathcal{C}_1$ and ciphertext space $\mathcal{C}_2$. Consider the following derived re-randomizable PKE scheme $\mathsf{E} = (\mathsf{E.Gen}, \mathsf{E.Enc}, \mathsf{E.Dec})$ with message space $\mathcal{M} = \mathcal{M}_1$ and ciphertext space $\mathcal{C} = \mathcal{C}_2$.

Key Generation: Upon input the security parameter $\lambda \in \mathbb{N}$, algorithm $\mathsf{E.Gen}(1^\lambda)$ runs $(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow^{\$} \mathsf{E.Gen}_1(1^\lambda)$ and $(\mathsf{pk}_2, \mathsf{sk}_2) \leftarrow^{\$} \mathsf{E.Gen}_2(1^\lambda)$ and outputs $\mathsf{pk} = (\mathsf{pk}_1, \mathsf{pk}_2)$ and $\mathsf{sk} = (\mathsf{sk}_1, \mathsf{sk}_2)$.

Encryption: Upon input the public key $\mathsf{pk} = (\mathsf{pk}_1, \mathsf{pk}_2)$ and a message $m \in \mathcal{M}$, algorithm $\mathsf{E.Enc}(\mathsf{pk}, m)$ lets $c_1 \leftarrow^{\$} \mathsf{E.Enc}_1(\mathsf{pk}_1, m)$ and outputs $c = c_2 \leftarrow^{\$} \mathsf{E.Enc}_2(\mathsf{pk}_2, c_1)$.

Decryption: Upon input the secret key $\mathsf{sk} = (\mathsf{sk}_1, \mathsf{sk}_2)$ and a ciphertext $c \in \mathcal{C}$, the decryption algorithm lets $c_1 = \mathsf{E.Dec}_2(\mathsf{sk}_2, c)$. If $c_1 = \perp$, it returns $\perp$. Else, it returns $m = \mathsf{E.Dec}_1(\mathsf{sk}_1, c_1)$.

Re-randomization: Upon input the public key $\mathsf{pk} = (\mathsf{pk}_1, \mathsf{pk}_2)$ and a ciphertext $c \in \mathcal{C}$, the re-randomization algorithm returns the same as $\mathsf{Rerand}(\mathsf{pk}_2, c)$.

Theorem 6. *Assuming that* E_1 *is* IND-CCA2 *secure and that* E_2 *is both* IND-CCA1 *secure and* RAND-CCA1 *secure (resp.* RAND-CPA *secure), the above defined PKE scheme* E *is both* IND-RCCA *secure and* RAND-CCA1 *secure (resp.* RAND-CPA *secure).*

Proof. The theorem follows directly by combining the two lemmas below.

Lemma 5. *Assuming that* E_1 *is* IND-CCA2 *secure, the PKE scheme* E *is* IND-RCCA *secure.*

Proof. By contradiction, assume there exists a PPT adversary $\mathcal{A}$ and a polynomial $p(\lambda)$ such that

$$\mathsf{Adv}^{\mathsf{rcca}}_{\mathsf{E},\mathcal{A}}(\lambda) \geq 1/p(\lambda).$$

Consider the following PPT adversary $\mathcal{A}_1$ attacking IND-CCA2 security of E_1:

- Upon receiving pk_1 from the challenger, sample $(\mathsf{pk}_2, \mathsf{sk}_2) \leftarrow^{\$} \mathsf{E.Gen}_2(1^\lambda)$ and forward $\mathsf{pk} = (\mathsf{pk}_1, \mathsf{pk}_2)$ to $\mathcal{A}$.
- Upon receiving a decryption query $c \in \mathcal{C} = \mathcal{C}_2$ from $\mathcal{A}$, let $c_1 = \mathsf{E.Dec}_2(\mathsf{sk}_2, c)$. If $c_1 = \perp$, return $\perp$ to $\mathcal{A}$. Else, forward c_1 to the challenger obtaining $m = \mathsf{E.Dec}_1(\mathsf{sk}_1, c_1) \in \mathcal{M} \cup \{\perp\}$ and return m to $\mathcal{A}$.
- Whenever $\mathcal{A}$ outputs (m_0, m_1) forward (m_0, m_1) to the challenger obtaining a ciphertext $c_1^* \leftarrow^{\$} \mathsf{E.Enc}_1(\mathsf{pk}_1, m_b)$ (where b is the challenge bit sampled by the challenger). Then, compute $c^* \leftarrow^{\$} \mathsf{E.Enc}_2(\mathsf{pk}_2, c_1^*)$.
- Upon receiving a decryption query $c \in \mathcal{C} = \mathcal{C}_2$ from $\mathcal{A}$, let $c_1 = \mathsf{E.Dec}_2(\mathsf{sk}_2, c)$. If $c_1 = \perp$, return $\perp$ to $\mathcal{A}$. Else, if $c_1 = c_1^*$ return $\diamond$ to $\mathcal{A}$. Else, forward c_1 to the challenger obtaining $m = \mathsf{E.Dec}_1(\mathsf{sk}_1, c_1) \in \mathcal{M} \cup \{\perp\}$ and return m to $\mathcal{A}$ unless $m \in \{m_0, m_1\}$ (in which case, return $\diamond$ to $\mathcal{A}$).
- Output whatever $\mathcal{A}$ outputs.

For the analysis, we note that $\mathcal{A}_1$ perfectly simulates the distribution of the public key $\mathsf{pk} = (\mathsf{pk}_1, \mathsf{pk}_2)$ and of the challenge ciphertext c^*. Additionally, decryption queries are also perfectly simulated using knowledge of the secret key sk_2 and oracle access to $\mathsf{E.Dec}_1(\mathsf{sk}_1, \cdot)$. This is immediate for decryption queries asked before the challenge. As for decryption queries asked after the challenge, observe that $\mathcal{A}_1$ is not allowed to query c_1^* to the decryption oracle; however, in case removing the outer encryption layer using secret key sk_2 yields a ciphertext $c_1 = c_1^*$, the reduction can answer to this query with $\diamond$. Furthermore, the reduction can efficiently check whether decryption of $c_1 \neq c_1^*$ yields a value in $\{m_0, m_1\}$, which yields a perfect simulation of oracle $\mathsf{E.Dec}^{\diamond}(\mathsf{sk}, m_0, m_1, \cdot)$. Hence: $\mathsf{Adv}^{\mathsf{cca}}_{\mathsf{E}_1,\mathcal{A}_1}(\lambda) \geq 1/p(\lambda)$ and the lemma follows. □

Lemma 6. *Assuming that* E_2 *is both* IND-CCA1 *secure and* RAND-CCA1 *secure (resp.* RAND-CPA *secure), the PKE scheme* E *is* RAND-CCA1 *secure (resp.* RAND-CPA *secure).*

Proof. We prove the lemma in the RAND-CCA1; the proof in the RAND-CPA case is identical except that we do not need to take into account decryption queries. We consider a sequence of hybrid experiments, defined below.

Hybrid $\mathcal{H}_0$: This is identical to experiment $\mathsf{RAND\text{-}CCA1}_{\mathsf{E},\mathcal{A}}(1^\lambda)$ with the challenge bit fixed to $b = 0$. In particular, the challenge ciphertext is computed as follows. Let $\widetilde{c}_1 = \mathsf{E.Dec}_2(\mathsf{sk}_2, \widetilde{c})$ and $\widetilde{m} = \mathsf{E.Dec}_1(\mathsf{sk}_1, \widetilde{c}_1)$. If either of $\widetilde{c}_1$ or $\widetilde{m} = \perp$, set $c^* = \perp$. Else, let $c^* \leftarrow^{\$} \mathsf{E.Enc}_2(\mathsf{pk}_2, \mathsf{E.Enc}_1(\mathsf{pk}_1, \widetilde{m}))$.

Hybrid $\mathcal{H}_0'$: This is identical to $\mathcal{H}_0$, except that we modify the distribution of the challenge ciphertext c^*. Let $\widetilde{c}_1 = \mathsf{E.Dec}_2(\mathsf{sk}_2, \widetilde{c})$ and $\widetilde{m} = \mathsf{E.Dec}_1(\mathsf{sk}_1, \widetilde{c}_1)$. If either of $\widetilde{c}_1$ or $\widetilde{m} = \perp$, set $c^* = \perp$ (as before); otherwise, $c^* \leftarrow^{\$} \mathsf{E.Enc}_2(\mathsf{pk}_2, \widetilde{c}_1)$.

Hybrid $\mathcal{H}_1$: This is identical to experiment $\mathsf{RAND\text{-}CCA1}_{\mathsf{E},\mathcal{A}}(1^\lambda)$ with the challenge bit fixed to $b = 1$. In particular, the challenge ciphertext is computed as follows. Let $\widetilde{c}_1 = \mathsf{E.Dec}_2(\mathsf{sk}_2, \widetilde{c})$ and $\widetilde{m} = \mathsf{E.Dec}_1(\mathsf{sk}_1, \widetilde{c}_1)$. If either of $\widetilde{c}_1$ or $\widetilde{m} = \bot$, set $c^* = \bot$ (as before). Else, let $c^* \leftarrow^{\$} \mathsf{Rerand}(pk_2, \widetilde{c}_1)$.

We first show that $\mathcal{H}_0 \approx_c \mathcal{H}'_0$. Towards this, let $\mathcal{D}$ be a PPT distinguisher telling apart the two experiments with distinguishing advantage $1/p(\lambda)$ for some polynomial $p(\lambda)$. We build a PPT attacker $\mathcal{A}_2$ breaking CCA1 security of E_2 as follows:

- Upon receiving pk_2 from the challenger, sample $(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow^{\$} \mathsf{E.Gen}_1(1^\lambda)$ and forward $\mathsf{pk} = (\mathsf{pk}_1, \mathsf{pk}_2)$ to $\mathcal{D}$.
- Upon receiving a decryption query $c \in \mathcal{C} = \mathcal{C}_2$ from $\mathcal{D}$, forward c to the challenger obtaining $c_1 = \mathsf{E.Dec}_2(\mathsf{sk}_2, c)$. If $c_1 = \bot$, return $\bot$ to $\mathcal{A}$. Else, let $m = \mathsf{E.Dec}_1(\mathsf{sk}_1, c_1) \in \mathcal{M} \cup \{\bot\}$ and return m to $\mathcal{D}$.
- Whenever $\mathcal{D}$ outputs a ciphertext $\widetilde{c}$, forward $\widetilde{c}$ to the challenger obtaining $\widetilde{c}_1 = \mathsf{E.Dec}_2(\mathsf{sk}_2, \widetilde{c})$. If $\widetilde{c}_1 = \bot$, return $\bot$ to $\mathcal{D}$. Else, let $\widetilde{m} = \mathsf{E.Dec}_1(\mathsf{sk}_1, \widetilde{c}_1) \in \mathcal{M} \cup \{\bot\}$. If $\widetilde{m} = \bot$, return $\bot$ to $\mathcal{D}$. Else, forward the challenge messages $(c_1, \widetilde{c}_1)$ to the challenger, where $c_1 \leftarrow^{\$} \mathsf{E.Enc}_1(\mathsf{pk}_1, \widetilde{m})$. Upon receiving c^* from the challenger forward it to $\mathcal{D}$.
- Output whatever $\mathcal{D}$ outputs.

For the analysis, we note that $\mathcal{A}_2$ perfectly simulates the distribution of the public key $\mathsf{pk} = (\mathsf{pk}_1, \mathsf{pk}_2)$. Additionally, decryption queries are also perfectly simulated using knowledge of the secret key sk_1 and oracle access to $\mathsf{E.Dec}_2(\mathsf{sk}_2, \cdot)$. As for the challenge ciphertext c^*, we observe that in case the IND-CCA1 challenger encrypts c_1 the distribution of c^* is identical to $\mathsf{E.Enc}_2(\mathsf{pk}_2, \mathsf{E.Enc}_1(\mathsf{pk}_1, m))$ as defined in $\mathcal{H}_0$. On the other hand, in case the IND-CCA1 challenger encrypts $\widetilde{c}_1$ the distribution of c^* is identical to $\mathsf{E.Enc}_2(\mathsf{pk}_2, \widetilde{c}_1)$ as defined in $\mathcal{H}'_0$ Hence, $\mathcal{A}_2$ breaks IND-CCA1 security with advantage $1/p(\lambda)$, a contradiction.

To finish the proof, it remains to show that $\mathcal{H}'_0 \approx_c \mathcal{H}_1$. By contradiction, assume there exists a PPT distinguisher $\mathcal{D}$ and a polynomial $p(\lambda)$ telling apart the two experiments with distinguishing advantage $1/p(\lambda)$ for some polynomial $p(\lambda)$. We build a PPT attacker $\mathcal{A}_2$ breaking RAND-CCA1 security of E_2 as follows:

- Upon receiving pk_2 from the challenger, sample $(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow^{\$} \mathsf{E.Gen}_1(1^\lambda)$ and forward $\mathsf{pk} = (\mathsf{pk}_1, \mathsf{pk}_2)$ to $\mathcal{D}$.
- Upon receiving a decryption query $c \in \mathcal{C} = \mathcal{C}_2$ from $\mathcal{D}$, forward c to the challenger obtaining $c_1 = \mathsf{E.Dec}_2(\mathsf{sk}_2, c)$. If $c_1 = \bot$, return $\bot$ to $\mathcal{A}$. Else, let $m = \mathsf{E.Dec}_1(\mathsf{sk}_1, c_1) \in \mathcal{M} \cup \{\bot\}$ and return m to $\mathcal{D}$.
- Whenever $\mathcal{D}$ outputs a ciphertext $\widetilde{c}$, forward $\widetilde{c}$ to the challenger obtaining $\widetilde{c}_1 = \mathsf{E.Dec}_2(\mathsf{sk}_2, \widetilde{c})$. If $\widetilde{c}_1 = \bot$, return $\bot$ to $\mathcal{D}$. Else, let $\widetilde{m} = \mathsf{E.Dec}_1(\mathsf{sk}_1, \widetilde{c}_1) \in \mathcal{M} \cup \{\bot\}$. If $\widetilde{m} = \bot$, return $\bot$ to $\mathcal{D}$. Else, forward $\widetilde{c}$ to the challenger. Upon receiving c^* from the challenger forward it to $\mathcal{D}$.
- Output whatever $\mathcal{D}$ outputs.

For the analysis, we note that $\mathcal{A}_2$ perfectly simulates the distribution of the public key $\mathsf{pk} = (\mathsf{pk}_1, \mathsf{pk}_2)$. Additionally, decryption queries are also perfectly simulated using knowledge of the secret key sk_1 and oracle access to $\mathsf{E.Dec}_2(\mathsf{sk}_2, \cdot)$. As

for the challenge ciphertext c^*, we observe that the reduction first checks using a decryption query that $\widetilde{c}_1 = \mathsf{E.Dec}_2(\mathsf{sk}_2, \widetilde{c}) \neq \perp$ and that $\widetilde{m} = \mathsf{E.Dec}_1(\mathsf{sk}_1, \widetilde{c}_1) \neq \perp$. Assuming this is the case, it forwards $\widetilde{c}$ to the RAND-CCA1 challenger. Now, in case the RAND-CCA1 challenger encrypts $\widetilde{c}_1$ the distribution of c^* is identical to $\mathsf{E.Enc}(\mathsf{pk}_2, \widetilde{c}_1)$ as defined in $\mathcal{H}'_0$. On the other hand, in case the RAND-CCA1 challenger re-randomizes $\widetilde{c}$ the distribution of c^* is identical to $\mathsf{Rerand}(\mathsf{pk}_2, \widetilde{c})$ as defined in $\mathcal{H}_1$ Hence, $\mathcal{A}_2$ breaks RAND-CCA1 security with advantage $1/p(\lambda)$, a contradiction. The lemma follows. □

□

5.2 Instantiations

Let us now show how to instantiate the building blocks required by Thm. 6. Let $\mathbb{G}$ be a cyclic group of prime order q with generator $g \in \mathbb{G}$. We take E_2 to be the Cramer-Shoup PKE scheme with $\mathcal{M} = \mathcal{M}_1 = \mathbb{G}$ and $\mathcal{C}_1 = \mathbb{G}^4$. As shown by Cramer and Shoup [16], such a PKE achieves CCA2 security under the DDH assumption in $\mathbb{G}$. In what follows, let us denote by $c_1 = (c_{1,1}, c_{1,2}, c_{1,3}, c_{1,4})$ the four elements of a ciphertext.

In order to instantiate E_2, we start with the Cramer-Shoup Lite PKE scheme with message space $\mathbb{G}$ and ciphertext space $\mathbb{G}^4$. Recall that in such a scheme, the encryption algorithm upon input a message $m \in \mathbb{G}$ returns:

$$c = (g_1^r, g_2^r, h_1^r \cdot m, h_2^r)\,,$$

where $r \leftarrow^{\$} \mathbb{Z}_q$, $\mathsf{pk} = (g_1, g_2, h_1, h_2) \in \mathbb{G}^4$ and $\mathsf{sk} = (x_1, y_1, x_2, y_2) \in \mathbb{Z}_q^4$ such that $h_1 = g_1^{x_1} \cdot g_2^{y_1}$ and $h_2 = g_1^{x2} \cdot g_2^{y_2}$. As shown by Cramer and Shoup [16], such a PKE achieves CCA1 security under the DDH assumption in $\mathbb{G}$; additionally, it is not hard to prove that the same PKE is re-randomizable and satisfies RAND-CCA1 security.

Now, we could encrypt each of the four group elements in c_1 independently using Cramer-Shoup Lite. This is still re-randomizable and yields ciphertexts consisting of 16 group elements. This can be improved by reusing randomness, as suggested by Bellare, Boldyreva and Staddon [4] in the context of multi-recipient PKE. In particular, we can take E_2 to be the following variant of Cramer-Shoup Lite with $\mathcal{M}_2 = \mathcal{C}_1 = \mathbb{G}^4$ and $\mathcal{C}_2 = \mathbb{G}^7$:

$$c_2 = (c_{2,1}, \ldots, c_{2,7}) = \left(g_1^r, g_2^r, \{h_1^r \cdot c_{1,j}\}_{j=1}^4, h_2^r\right),$$

where $r \leftarrow^{\$} \mathbb{Z}_q$, $\mathsf{pk}_2 = (g_1, g_2, h_1, h_2) \in \mathbb{G}^4$ and $\mathsf{sk}_2 = (x_1, y_1, x_2, y_2) \in \mathbb{Z}_q^4$ such that $h_1 = g_1^{x_1} \cdot g_2^{y_1}$ and $h_2 = g_1^{x2} \cdot g_2^{y_2}$. The above still satisfies CCA1 security, as well as RAND-CCA1 security with re-randomization algorithm:

$$\mathsf{Rerand}_2(\mathsf{pk}_2, c_2) = \left(c_{2,1} \cdot g_1^{r'}, c_{2,2} \cdot g_2^{r'}, \{c_{2,j} \cdot h_1^{r'}\}_{j=3}^6, c_{2,7} \cdot h_2^{r'}\right).$$

The above yields ciphertexts consisting of 7 group elements under the DDH assumption in the plain model (with public keys consisting of 6 group elements and secret keys consisting of 8 elements in $\mathbb{Z}_q$).

References

1. Gennaro Avitabile, Vincenzo Botta, Emanuele Giunta, Marcin Mielniczuk, and Francesco Migliaro. The malice of ELFs: Practical anamorphic-resistant encryption without random oracles. In Joan Daemen and Emmanuel Thomé, editors, *EUROCRYPT 2026, Part V*, volume 16545 of *LNCS*, pages 303–333. Springer, Cham, May 2026.
2. Fabio Banfi, Konstantin Gegier, Martin Hirt, Ueli Maurer, and Guilherme Rito. Anamorphic encryption, revisited. In Marc Joye and Gregor Leander, editors, *EUROCRYPT 2024, Part II*, volume 14652 of *LNCS*, pages 3–32. Springer, Cham, May 2024.
3. Mihir Bellare, Alexandra Boldyreva, and Adam O'Neill. Deterministic and efficiently searchable encryption. In Alfred Menezes, editor, *CRYPTO 2007*, volume 4622 of *LNCS*, pages 535–552. Springer, Berlin, Heidelberg, August 2007.
4. Mihir Bellare, Alexandra Boldyreva, and Jessica Staddon. Randomness re-use in multi-recipient encryption schemeas. In Yvo Desmedt, editor, *PKC 2003*, volume 2567 of *LNCS*, pages 85–99. Springer, Berlin, Heidelberg, January 2003.
5. Mihir Bellare, Kenneth G. Paterson, and Phillip Rogaway. Security of symmetric encryption against mass surveillance. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 1–19. Springer, Berlin, Heidelberg, August 2014.
6. Alexandra Boldyreva, Serge Fehr, and Adam O'Neill. On notions of security for deterministic encryption, and efficient constructions without random oracles. In David Wagner, editor, *CRYPTO 2008*, volume 5157 of *LNCS*, pages 335–359. Springer, Berlin, Heidelberg, August 2008.
7. Zvika Brakerski and Gil Segev. Better security for deterministic public-key encryption: The auxiliary-input setting. In Phillip Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 543–560. Springer, Berlin, Heidelberg, August 2011.
8. Ran Canetti, Hugo Krawczyk, and Jesper Buus Nielsen. Relaxing chosen-ciphertext security. In Dan Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 565–582. Springer, Berlin, Heidelberg, August 2003.
9. Davide Carnemolla, Dario Catalano, Emanuele Giunta, and Francesco Migliaro. Anamorphic resistant encryption: the good, the bad and the ugly. In Yael Tauman Kalai and Seny F. Kamara, editors, *CRYPTO 2025, Part III*, volume 16002 of *LNCS*, pages 472–503. Springer, Cham, August 2025.
10. Dario Catalano, Emanuele Giunta, and Francesco Migliaro. Anamorphic encryption: New constructions and homomorphic realizations. In Marc Joye and Gregor Leander, editors, *EUROCRYPT 2024, Part II*, volume 14652 of *LNCS*, pages 33–62. Springer, Cham, May 2024.
11. Dario Catalano, Emanuele Giunta, and Francesco Migliaro. Limits of black-box anamorphic encryption. In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part II*, volume 14921 of *LNCS*, pages 352–383. Springer, Cham, August 2024.
12. Dario Catalano, Emanuele Giunta, and Francesco Migliaro. Generic anamorphic encryption, revisited: New limitations and constructions. In Serge Fehr and Pierre-Alain Fouque, editors, *EUROCRYPT 2025, Part II*, volume 15602 of *LNCS*, pages 275–303. Springer, Cham, May 2025.
13. Seung Geol Choi, Dana Dachman-Soled, Tal Malkin, and Hoeteck Wee. Black-box construction of a non-malleable encryption scheme from any semantically secure one. In Ran Canetti, editor, *TCC 2008*, volume 4948 of *LNCS*, pages 427–444. Springer, Berlin, Heidelberg, March 2008.

14. Wonseok Choi, Daniel Collins, Xiangyu Liu, Roy Stracovsky, and Vassilis Zikas. A unified treatment of anamorphic encryption. In *Advances in Cryptology – CRYPTO 2026*, 2026.
15. Sandro Coretti, Yevgeniy Dodis, Björn Tackmann, and Daniele Venturi. Non-malleable encryption: Simpler, shorter, stronger. In Eyal Kushilevitz and Tal Malkin, editors, *TCC 2016-A, Part I*, volume 9562 of *LNCS*, pages 306–335. Springer, Berlin, Heidelberg, January 2016.
16. Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In Hugo Krawczyk, editor, *CRYPTO'98*, volume 1462 of *LNCS*, pages 13–25. Springer, Berlin, Heidelberg, August 1998.
17. Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In Lars R. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 45–64. Springer, Berlin, Heidelberg, April / May 2002.
18. Xuan Thanh Do, Giuseppe Persiano, Duong Hieu Phan, and Moti Yung. Anamorphism beyond one-to-one messaging: Public-key with anamorphic broadcast mode. In Serge Fehr and Pierre-Alain Fouque, editors, *EUROCRYPT 2025, Part III*, volume 15603 of *LNCS*, pages 429–455. Springer, Cham, May 2025.
19. Yevgeniy Dodis and Eli Goldin. Anamorphic-resistant encryption; or why the encryption debate is still alive. In Yael Tauman Kalai and Seny F. Kamara, editors, *CRYPTO 2025, Part III*, volume 16002 of *LNCS*, pages 440–471. Springer, Cham, August 2025.
20. Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In G. R. Blakley and David Chaum, editors, *CRYPTO'84*, volume 196 of *LNCS*, pages 10–18. Springer, Berlin, Heidelberg, August 1984.
21. Antonio Faonio and Dario Fiore. Improving the efficiency of re-randomizable and replayable CCA secure public key encryption. In Mauro Conti, Jianying Zhou, Emiliano Casalicchio, and Angelo Spognardi, editors, *ACNS 2020, Part I*, volume 12146 of *LNCS*, pages 271–291. Springer, Cham, October 2020.
22. Antonio Faonio, Dario Fiore, Javier Herranz, and Carla Ràfols. Structure-preserving and re-randomizable RCCA-secure public key encryption and its applications. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part III*, volume 11923 of *LNCS*, pages 159–190. Springer, Cham, December 2019.
23. Jens Groth. Rerandomizable and replayable adaptive chosen ciphertext attack secure cryptosystems. In Moni Naor, editor, *TCC 2004*, volume 2951 of *LNCS*, pages 152–170. Springer, Berlin, Heidelberg, February 2004.
24. Joseph Jaeger and Roy Stracovsky. Dictators? Friends? Forgers. - breaking and fixing unforgeability definitions for anamorphic signature schemes. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024, Part II*, volume 15485 of *LNCS*, pages 105–137. Springer, Singapore, December 2024.
25. Venkata Koppula and Brent Waters. Realizing chosen ciphertext security generically in attribute-based encryption and predicate encryption. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 671–700. Springer, Cham, August 2019.
26. Miroslaw Kutylowski, Giuseppe Persiano, Duong Hieu Phan, Moti Yung, and Marcin Zawada. Anamorphic signatures: Secrecy from a dictator who only permits authentication! In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part II*, volume 14082 of *LNCS*, pages 759–790. Springer, Cham, August 2023.

27. Miroslaw Kutylowski, Giuseppe Persiano, Duong Hieu Phan, Moti Yung, and Marcin Zawada. The self-anti-censorship nature of encryption: On the prevalence of anamorphic cryptography. *PoPETs*, 2023(4):170–183, October 2023.
28. Bodo Möller. A public-key encryption scheme with pseudo-random ciphertexts. In Pierangela Samarati, Peter Y. A. Ryan, Dieter Gollmann, and Refik Molva, editors, *ESORICS 2004*, volume 3193 of *LNCS*, pages 335–351. Springer, Berlin, Heidelberg, September 2004.
29. Moni Naor and Moti Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *22nd ACM STOC*, pages 427–437. ACM Press, May 1990.
30. Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In Jacques Stern, editor, *EUROCRYPT'99*, volume 1592 of *LNCS*, pages 223–238. Springer, Berlin, Heidelberg, May 1999.
31. Rafael Pass, abhi shelat, and Vinod Vaikuntanathan. Construction of a non-malleable encryption scheme from any semantically secure one. In Cynthia Dwork, editor, *CRYPTO 2006*, volume 4117 of *LNCS*, pages 271–289. Springer, Berlin, Heidelberg, August 2006.
32. Giuseppe Persiano, Duong Hieu Phan, and Moti Yung. Anamorphic encryption: Private communication against a dictator. In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part II*, volume 13276 of *LNCS*, pages 34–63. Springer, Cham, May / June 2022.
33. Giuseppe Persiano, Duong Hieu Phan, and Moti Yung. Public-key anamorphism in (CCA-secure) public-key encryption and beyond. In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part II*, volume 14921 of *LNCS*, pages 422–455. Springer, Cham, August 2024.
34. Duong Hieu Phan and David Pointcheval. OAEP 3-round: A generic and secure asymmetric encryption padding. In Pil Joong Lee, editor, *ASIACRYPT 2004*, volume 3329 of *LNCS*, pages 63–77. Springer, Berlin, Heidelberg, December 2004.
35. Manoj Prabhakaran and Mike Rosulek. Rerandomizable RCCA encryption. In Alfred Menezes, editor, *CRYPTO 2007*, volume 4622 of *LNCS*, pages 517–534. Springer, Berlin, Heidelberg, August 2007.
36. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *37th ACM STOC*, pages 84–93. ACM Press, May 2005.
37. Amit Sahai. Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security. In *40th FOCS*, pages 543–553. IEEE Computer Society Press, October 1999.
38. Weihao Wang, Shuai Han, and Shengli Liu. Anamorphic authenticated key exchange: Double key distribution under surveillance. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024, Part V*, volume 15488 of *LNCS*, pages 168–200. Springer, Singapore, December 2024.
39. Yi Wang, Rongmao Chen, Xinyi Huang, and Moti Yung. Sender-anamorphic encryption reformulated: Achieving robust and generic constructions. In Jian Guo and Ron Steinfeld, editors, *ASIACRYPT 2023, Part VI*, volume 14443 of *LNCS*, pages 135–167. Springer, Singapore, December 2023.
40. Hoeteck Wee. Dual projective hashing and its applications - lossy trapdoor functions and more. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 246–262. Springer, Berlin, Heidelberg, April 2012.

A Additional Definitions

A.1 IND-CCA2 Secure Encryption

Definition 20 (IND-CCA2 Secure Encryption). *A public-key encryption scheme* $\mathsf{E} = (\mathsf{E.Gen}, \mathsf{E.Enc}, \mathsf{E.Dec})$ *is* IND-CCA2 secure *(indistinguishable under chosen-ciphertext attacks) if for all* PPT *adversaries* $\mathcal{A}$*, it holds that:*

$$\mathsf{Adv}^{\mathsf{IND\text{-}CCA2}}_{\mathsf{E},\mathcal{A}}(\lambda) := \left|\Pr[\mathsf{IND\text{-}CCA2}^{\mathcal{A}}_{\mathsf{E}}(1^\lambda) = 1] - \frac{1}{2}\right| \leq \mathsf{negl}(\lambda)$$

where the IND-CCA2 *game is defined in Fig. 17.*

$\mathsf{IND\text{-}CCA2}^{\mathcal{A}}_{\mathsf{E}}(1^\lambda)$

1 : $(\mathsf{pk}, \mathsf{sk}) \leftarrow^{\$} \mathsf{E.Gen}(1^\lambda)$
2 : $(m_0, m_1, \mathrm{st}) \leftarrow^{\$} \mathcal{A}^{\mathsf{E.Dec}(\mathsf{sk},\cdot)}(\mathsf{pk})$
3 : $b \leftarrow^{\$} \{0,1\}$
4 : $c^* \leftarrow^{\$} \mathsf{E.Enc}(\mathsf{pk}, m_b)$
5 : $b' \leftarrow^{\$} \mathcal{A}^{\mathsf{E.Dec}^*(\mathsf{sk},\cdot)}(\mathrm{st}, c^*)$
6 : **return** $b = b'$

Fig. 17. IND-CCA2 security game. $\mathsf{E.Dec}^*(\mathsf{ask}, \cdot)$ behaves as $\mathsf{E.Dec}(\mathsf{ask}, \cdot)$ with the exception that it refuses to decrypt the challenge ciphertext c^*.

If the adversary can access the decryption oracle only up until the point that it receives a challenge ciphertext the property is called IND-CCA1.

A.2 Non-Malleable Encryption

We recall the notion of non-malleability under chosen-plaintext attacks of [31].

Definition 21 (Non-Malleable Encryption). *A public-key encryption scheme* $\mathsf{E} = (\mathsf{E.Gen}, \mathsf{E.Enc}, \mathsf{E.Dec})$ *is* NM-CPA secure *(non-malleable under chosen-plaintext attacks) if for* $\ell \in \mathbb{N}$ *and for all* PPT *adversaries* $\mathcal{A}$*, it holds that:*

$$\mathsf{Adv}^{\mathsf{NM\text{-}CPA}}_{\mathsf{E},\mathcal{A},\ell}(\lambda) := \left|\Pr[\mathsf{NM\text{-}CPA}^{\mathcal{A}}_{\mathsf{E},\ell}(1^\lambda, 0) = 1] - \Pr[\mathsf{NM\text{-}CPA}^{\mathcal{A}}_{\mathsf{E},\ell}(1^\lambda, 1) = 1]\right| \leq \mathsf{negl}(\lambda)$$

where the NM-CPA *game is defined in Fig. 18.*

It is easy to observe that IND-CCA2 $\implies$ NM-CPA.

$\mathsf{NM\text{-}CPA}^{\mathcal{A}}_{\mathsf{E},\ell}(1^\lambda, b)$

$(\mathsf{pk}, \mathsf{sk}) \leftarrow^{\$} \mathsf{E.Gen}(1^\lambda)$
$(m_0, m_1) \leftarrow^{\$} \mathcal{A}(\mathsf{pk})$
$c^* \leftarrow^{\$} \mathsf{E.Enc}(\mathsf{pk}, m_b)$
$(c_1, \ldots, c_\ell) \leftarrow^{\$} \mathcal{A}(c^*)$
for $i \in \{1, \ldots, \ell\}$
  if $c_i == c^*$ **then**
    $d_i = \perp$
  else
    $d_i = \mathsf{E.Dec}(\mathsf{sk}, c_i)$
return $\mathcal{A}(d_1, \ldots, d_\ell)$

Fig. 18. NM-CPA security game.

$\mathsf{Robust}^b_{\mathsf{E},\mathsf{AT},\mathcal{A}}(\lambda)$

$((\mathsf{apk}, \mathsf{ask}), \mathsf{dk}, \mathsf{tk}) \leftarrow^{\$} \mathsf{AT.Gen}(\lambda)$
return $\mathcal{A}^{\mathcal{O}^b(\mathsf{apk},\mathsf{ask},\mathsf{dk},\mathsf{tk},\cdot)}(\mathsf{apk}, \mathsf{ask})$ where
  $\mathcal{O}^0(\mathsf{apk}, \mathsf{ask}, \mathsf{dk}, \mathsf{tk}, m) = \mathsf{AT.Dec}(\mathsf{tk}, \mathsf{ask}, \mathsf{E.Enc}(\mathsf{apk}, m))$
  $\mathcal{O}^1(\mathsf{apk}, \mathsf{ask}, \mathsf{dk}, \mathsf{tk}, m) = \perp$

Fig. 19. Anamorphic Encryption Robustness game.

A.3 Robustness of AE

Let E be a PKE scheme equipped with an Anamorphic Triplet AT. We define the robustness game, for $b \in \{0, 1\}$, in Fig. 19.

And we define the advantage of an adversary $\mathcal{A}$ in breaking the robustness property as

$$\mathsf{Adv}^{\mathsf{rob}}_{\mathsf{E},\mathsf{AT},\mathcal{A}}(\lambda) := \left|\Pr\left[\mathsf{Robust}^0_{\mathsf{E},\mathsf{AT},\mathcal{A}}(\lambda) = 1\right] - \Pr\left[\mathsf{Robust}^1_{\mathsf{E},\mathsf{AT},\mathcal{A}}(\lambda) = 1\right]\right|.$$

Definition 22 (Robustness). *An Anamorphic Encryption scheme* E *equipped with Anamorphic Triplet* AT *is said to be robust if for all* PPT *adversary* $\mathcal{A}$ *it holds that*

$$\mathsf{Adv}^{\mathsf{rob}}_{\mathsf{E},\mathsf{AT},\mathcal{A}}(\lambda) \leq \mathsf{negl}(\lambda).$$