Residuosity-Based Efficient Anamorphic Extension: New Constructions and Security Analysis

Nabanita Chakraborty[1*†] and Ratna Dutta[1†]

[1*]Department of Mathematics, Indian Institute of Technology Kharagpur, Kharagpur, West Midnapore, 721302, West Bengal, India.

*Corresponding author(s). E-mail(s): nabanita@kgpian.iitkgp.ac.in;
Contributing authors: ratna@maths.iitkgp.ac.in;
†These authors contributed equally to this work.

Abstract

Anamorphic encryption (AE) enables covert communication in adversarial settings where the receiver's secret key may be exposed to a coercive adversary. Although existing AE constructions demonstrate the feasibility of this paradigm, their covert bandwidth rates are severely limited, particularly when built from conventional *public-key encryption* (PKE) schemes. This work develops a systematic approach to constructing *bandwidth-efficient anamorphic extensions* of *residuosity-based PKEs*.

We first present a *robust* bit-wise anamorphic extension of the *Goldwasser-Micali cryptosystem* and a *block variant* that substantially improves covert throughput. We then construct an anamorphic extension of the *Benaloh cryptosystem* using an explicit, uniquely decodable embedding of covert messages together with a redundancy tag for robustness. Beyond individual constructions, we introduce a general $\mathbf{\Delta}$*-structured public-key encryption framework* that captures the common algebraic structure enabling anamorphic extensions and instantiate it with *block Goldwasser-Micali*, *Paillier* and *Damgård-Jurik encryption*. We further provide a formal analysis of key deniability, robustness, message loss and windowed decryption, counter-reuse attacks, and forward security against subsequent sender coercion. The security of our constructions is established through *indistinguishability between normal and anamorphic mode* (IND-NA) reductions to *pseudorandom-function security*. At the *128-bit security level*, our Benaloh, block Goldwasser-Micali and Paillier constructions achieve approximately **0.46-0.48 covert bits per ciphertext bit** under the comparison metric considered, demonstrating a substantial bandwidth improvement over the representative prior approaches. Overall, the proposed framework provides a unified foundation

for designing efficient anamorphic extensions of structured public-key encryption schemes.

Keywords: Pseudorandom function, Anamorphic extension, Goldwasser-Micali PKE, Benaloh PKE, Paillier PKE, Damgård-Jurik PKE, IND-NA security, Key deniability, Robustness

MSC Classification: 11T71 , 94A60 , 68P25 , 68P27 , 68P30

1 Introduction

The fundamental objective of cryptography has always been to guarantee secure communication between legitimate users over inherently insecure channels, despite the presence of potential eavesdroppers. In the contemporary, technologically driven world, however, a critical question frequently arises from governmental and regulatory bodies:

To what extent should individual privacy be permitted?

While absolute privacy ensures strong protection for users, it can also be exploited by malicious actors such as terrorists or adversarial entities to endanger public safety. Consequently, governments often reserve the authority to oversee or regulate the privacy of their citizens to mitigate such risks. Yet, this concentration of power may, in certain circumstances, foster authoritarian control, wherein governing authorities can compel users to disclose their secret keys, thereby gaining unrestricted access to all private communications. To preserve individual privacy under such potentially oppressive conditions, covert communication techniques - notably anamorphic encryption - have emerged as promising cryptographic mechanisms. These techniques enable secure and deniable information exchange, even in environments where privacy is subject to intrusive governmental oversight.

1.1 Application Scenario

The application scenario of an AE is depicted in Fig. 1. In a PKE, the receiver generates its secret and public key pair $(\mathsf{sk}, \mathsf{pk})$ by running the key-generation algorithm on the input of the public parameters pp. Any sender can encrypt a message M using pp and the public key pk of the receiver and send the corresponding ciphertext ct to the receiver through an insecure channel. However, in the dictatorial setup, the dictator has access to sk and can decrypt all ciphertexts encrypted under pk. So, to enable secure communication in such a situation, the sender does the following

- runs an anamorphic setup algorithm using pk of the receiver and sets the anamorphic parameters ap (this step needs only public input and can be run by any party).
- generates a double key dk and a counter ctr by running anamorphic key generation algorithm on input ap and pk.
- sends $(\mathsf{ap}, \mathsf{dk}, \mathsf{ctr})$ to the receiver securely.

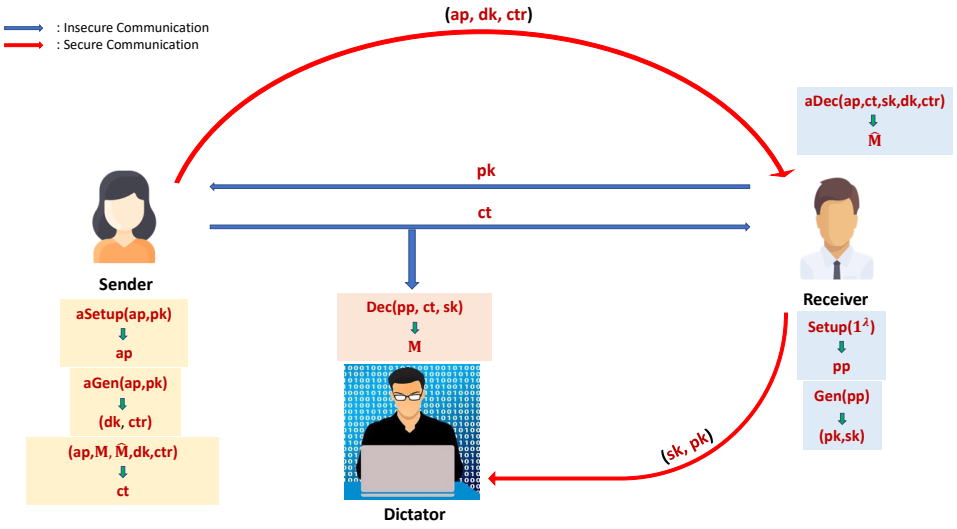


Fig. 1 Anamorphic Communication in the presence of a dictator

- encrypts a normal message M and a covert message $\widehat{\mathsf{M}}$ running the anamorphic encryption algorithm using ap, dk and ctr, generates the anamorphic ciphertext ct and updates the counter ctr by a rule.
- sends to the receiver through an insecure channel.

The receiver anamorphically decrypts the ciphertext ct using ap, dk and ctr, gets the covert message $\widehat{\mathsf{M}}$ and updates the counter with the same rule as the sender. The dk and ctr are established once during the anamorphic key-generation, after which the sender and receiver keep their counters synchronized by the same deterministic update rule for all subsequent anamorphic communications. Since the dictator may drop, delay or reorder ciphertexts, the receiver may use a decryption window (Section 5). Note that normal decryption of the anamorphic ciphertext ct using pp and sk will only return the normal message M. Therefore, the dictator, endowed with sk, can recover the normal message M but not the covert message $\widehat{\mathsf{M}}$ due to lack of dk and ctr.

1.2 Literature Review

To provide privacy in spite of presence of a dictatorial authority who can access the receiver's secret key, Persiano et al. [1] proposed the novel paradigm of *anamorphic public key encryption* (APKE) in the year of 2022. They introduced two generic constructions of receiver APKE. The first one relies on *rejection sampling* supporting very small covert plaintext while the second one is constructed using *Naor-Yung transform* [2] which uses an NIZK proof system. However, this approach suffers from the limitation that the double key can be generated a single time, only in conjunction with a newly generated public-secret key pair. Whenever the receiver wants a

shift to anamorphic mode from normal mode, it needs to update its existing key-pair which is potentially suspicious to the dictator. To overcome this issue, Banfi et al. [3] in 2024, proposed the novel concept of *anamorphic extension* (AE) of several existing PKEs, enabling a user to correspond many double keys to a single existing key-pair of the receiver. The AE additionally features deniability where the receiver can plausibly deny ownership of a given double key as it is derived solely from the receiver's public key. The concept of robustness was introduced in their work which ensures that the anamorphic decryption of normally encrypted plaintext returns a decryption failure instead of returning a garbage covert plaintext, unlike [1]. They construct AE of ElGamal [4], Cramer-Shoup [5] and OAEP [6] encryption using *selective randomness recoverability* (SRR) property. In 2024, Catalano et al. [7] extended two generic and well-known encryption classes namely, hybrid encryption and the *identity-based encryption* (IBE)-to-*indistinguishable under chosen-ciphertext attacks* (IND-CCA) transform to support anamorphism. More importantly, they have proposed the notion of homomorphic anamorphic encryption where homomorphic properties hold for the covert plaintext as well as the normal one and given concrete instantiations. Later in 2025, Catalano et al. [8] demonstrated that the rejection sampling-based APKE becomes insecure when instantiated over a (contrived, yet IND-CPA secure) PKE scheme. More broadly, they showed an impossibility result, showing that *stateless* black-box APKE *cannot* achieve full security where stateless refers to unsynchronized setting. Persiano et al. [9] in 2024, proposed an APKE from the IND-CCA secure *Koppula-Waters* (KW) scheme. Dodis and Goldin [10] proposed the notion of *anamorphic-resistant* (AR) encryption, together with corresponding constructions and formal security definitions. They have shown that, within such schemes, any attempt to realize covert communication is either information-theoretically impossible or computationally infeasible. Carnemolla et al. [11] provided concrete instantiations of AR encryption schemes and established that APKE is equivalent to algorithm-substitution attacks under suitable conditions. Kutylowski et al. [12] demonstrated that several widely deployed PKEs, including Goldwasser-Micali, Paillier and RSA-OAEP, admit randomness recovery and are therefore anamorphic under the general construction. Chakraborty and Dutta [13] proposed the AE from the Blum-Goldwasser PKE. Banerjee et al. [14] proposed asymmetric anamorphic constructions from ElGamal and Dual Regev PKE along with several anamorphic signature schemes and introduced anamorphic constructions in the identity-based setup. Kutylowski et al. [12] also introduced anamorphic signatures.

1.3 Our Contribution

This paper aims to construct anamorphic versions of well-known residuosity-based PKEs that carry covert payloads at a meaningful rate when measured per ciphertext bit, have a small double key and low computational cost, are computationally robust and key-deniable in a formally defined sense and remain usable on a lossy network.
In spite of addressing the super-powerful dictatorial adversary, the existing schemes face the following challenges.

- The rejection-sampling construction of [1] has a very low bandwidth rate, the Naor-Yung one needs a simulation-sound NIZK and a large double key and the constructions of [3, 7, 9, 12] embed covert plaintexts that are small compared with the ciphertext.
- The schemes of [1, 7, 9, 12] do not guarantee *computational robustness*, that is, the anamorphic decryption of a normal ciphertext returns a meaningless covert plaintext instead of a decryption failure.
- Deniability is claimed for synchronized extensions, but it has not been formalized and the stateful nature of such extensions (message loss, reordering, state rollback, sender coercion) has not been analysed.

We present AEs of the Goldwasser-Micali cryptosystem [15] and the Benaloh cryptosystem [16], a formal treatment of the issues mentioned above and a framework that extends both ideas to further residuosity-based PKEs [17, 18].

1.3.1 Metrics

Let $|\mathsf{M}|$, $|\widehat{\mathsf{M}}|$ and $|\mathsf{ct}|$ be the bit lengths of the normal plaintext, the covert plaintext and the ciphertext. We use the *bandwidth rate* $\alpha = |\widehat{\mathsf{M}}|/|\mathsf{M}|$, the *ciphertext expansion rate* $\beta = |\mathsf{ct}|/|\mathsf{M}|$, the *anamorphic ciphertext expansion rate* $\gamma = |\mathsf{ct}|/|\widehat{\mathsf{M}}| = \beta/\alpha$ and its inverse, the *covert rate* $\varrho = |\widehat{\mathsf{M}}|/|\mathsf{ct}|$ (covert bits per ciphertext bit). The bandwidth rate α alone is misleading for bit-wise schemes, because a single normal bit already occupies a whole group element; γ and ϱ are the quantities that decide how much ciphertext traffic a covert message costs. All of these are used with these definitions throughout the paper, including the tables.

1.3.2 AE of Goldwasser Micali PKE

The Goldwasser Micali PKE [15] is a classical bit-wise PKE associated with the plaintext space $\mathcal{M} = \{0,1\}^n$ and ciphertext space $\mathcal{C} = \mathbb{Z}_N^n$ where $\mathbb{Z}_N$ is the additive group of integers modulo N and $\mathbb{Z}_N^n$ is the collection of all n-tuples over $\mathbb{Z}_N$.

- We give an anamorphic extension Π_{aGM} associated with the covert plaintext space $\widehat{\mathcal{M}} = \{0,1\}^n$. The covert bit $\widehat{m}_i$ is carried by which of two PRF outputs, selected by $m_i \oplus \widehat{m}_i$, is used as the encryption randomness of the i-th bit.
- The bit-wise structure enables natural *computational robustness* without any compromise in the size of the covert plaintext ($\alpha = 1$). More generally, we claim that *the bit-wise PKEs with recoverable randomness admit AEs that are robust and have bandwidth rate* 1.
- The double key is a single ν-bit PRF key ($\nu = 128$ suffices), so $|\mathsf{dk}| = \nu$ plus the public key.
- Its covert rate is only $\varrho = 1/\log_2 N$. The block variant of Section 6 removes this limitation.

1.3.3 AE of Benaloh cryptosystem

The Benaloh cryptosystem [16], associated with the plaintext space $\mathcal{M} = \mathbb{Z}_r$ and ciphertext space $\mathcal{C} = \mathbb{Z}_N^*$ where $N = pq$ for p, q being large primes such that $r \mid$

$(p-1), r \nmid (q-1), r^2 \nmid (p-1)$ for a prime r, has a ciphertext whose randomness component is an arbitrary element of $\Delta_r = \{a^r \mid a \in \mathbb{Z}_N^*\}$.

- We give Π_{aBen} with covert plaintext space $\widehat{\mathcal{M}} = \{0,1\}^\ell$ for $\ell = \lambda - 2 - \tau$ (where λ is the security parameter and τ is the size of redundancy tag) and an explicit injective embedding of bit strings into Δ_r with a unique and efficient decoding (Lemma 5).
- A τ-bit redundancy tag makes the extension computationally robust (false-acceptance probability $\leq 2^{-\tau-1}$).
- The covert rate is $\varrho = \ell / \log_2 N \approx 0.46$ and $\gamma \approx 2.2$ at $|N| = 3072$. The bandwidth rate $\alpha = \ell / \log_2 r$ is large because r must be small.
- The double key is a ν-bit PRF key.

1.3.4 Deniability, windowed decryption and forward-security

We define *key deniability* formally and prove it for all our schemes (Section 5). We add windowed decryption for lossy networks, show that counter reuse (state rollback) breaks IND-NA security and give a forward-secure variant for the case that a sender is coerced after the fact.
We also prove that the anamorphic mode is IND-CPA secure, the IND-NA security holds with many double keys and we state precisely what is *not* covered (active attacks).

1.3.5 Framework and new schemes

We define Δ-structured PKEs and a generic AE with correctness, robustness and IND-NA security proofs (Section 6). Instances are the *block Goldwasser-Micali AE* Π_{aGMb} ($\lambda - 2 - \tau$ covert bits per ciphertext element instead of one), the *Paillier AE* Π_{aPai} from the Paillier PKE [17] and its Damgård-Jurik generalization from Damgård-Jurik cryptosystem [18]. The framework turns the paper from two instantiations into a method; Okamoto-Uchiyama [19] and Naccache-Stern [20] need other embeddings and are left open.

1.3.6 Computational efficiencies

The operation counts are in Table 1.

1.4 Comparison

In this section, we compare our constructions with existing ones in Table 2 (structure: state, key, deniability, robustness), Table 3 (sizes and rates, symbolic) and Table 4 (concrete sizes at the 128-bit security level). The synchronized schemes (S in Table 2) are the right comparison class for ours; stateless schemes (L) cannot be fully secure in a black-box way [8] and are listed for context only.

- The rejection sampling-based construction of [1] lacks efficiency and offers a low bandwidth rate of $\frac{\log \lambda}{\lambda}$ for security parameter λ.
- The Naor-Yung transform-based construction of [1] with the bandwidth rate 1 employs a generic simulation-sound NIZK proof system that is not cost-efficient.

Table 1 Operation counts of the proposed AE schemes

Scheme	Enc
Π_{aGM}	$n(1\lvert\mathsf{PRF}\rvert + 2\rvert \times \rvert)$
Π_{aGMb}	$n(1\lvert\mathsf{PRF}\rvert + 3\rvert \times \rvert)$
Π_{aBen}	$1\lvert\mathsf{PRF}\rvert + 2\rvert \times \rvert + 2\lvert\mathsf{Exp}_r\rvert$
Π_{aPai}	$1\lvert\mathsf{PRF}\rvert + 2\rvert \times \rvert + 1\lvert\mathsf{Exp}_N\rvert$
Scheme	Dec
Π_{aGM}	$1\lvert\mathsf{Inv}\rvert + n(1\lvert L\rvert + \leq 2\lvert\mathsf{PRF}\rvert + \leq 3\rvert \times \rvert)$
Π_{aGMb}	$1\lvert\mathsf{Inv}\rvert + n(1\lvert L\rvert + 1\lvert\mathsf{Sqrt}_q\rvert + 1\lvert\mathsf{PRF}\rvert + 1\lvert\mathsf{Inv}_q\rvert + 3\rvert \times \rvert)$
Π_{aBen}	$1\lvert\mathsf{Exp}\rvert + \lvert\mathsf{DL}_r\rvert + 1\lvert\mathsf{Exp}_r\rvert + 1\lvert\mathsf{Exp}_q\rvert + 1\lvert\mathsf{PRF}\rvert + 2\rvert \times \rvert + 1\lvert\mathsf{Inv}_q\rvert$
Π_{aPai}	$2\lvert\mathsf{Exp}\rvert + 1\lvert\mathsf{PRF}\rvert + 3\rvert \times \rvert + 1\lvert\mathsf{Inv}\rvert$

n: number of normal plaintext bits in Π_{aGM}, Π_{aGMb}, $|\mathsf{PRF}|$: one PRF evaluation, $|\times|$: modular multiplication, $|\mathsf{Exp}|$: modular exponentiation with a full-size exponent, $|\mathsf{Exp}_r|$, $|\mathsf{Exp}_N|$: exponentiation with an exponent of $\log r$ resp. $\log N$ bits, $|\mathsf{Exp}_q|$, $|\mathsf{Inv}_q|$, $|\mathsf{Sqrt}_q|$: operations modulo the prime q, $|L|$: Legendre symbol modulo p, $|\mathsf{Inv}|$: modular inverse, $|\mathsf{DL}_r|$: discrete logarithm in a group of order r ($\leq r$ multiplications by scanning, $O(\sqrt{r})$ by baby-step giant-step, one lookup with a precomputed table). Sampling, additions and XORs are not counted.

The double key is large as it contains a common reference string for the underlying NIZK along with two public keys and one secret key of a generic PKE.

- The anamorphic construction of [9] from Koppula-Waters (KW) IND-CCA secure PKE uses hinting PRF and a generic IND-CPA secure PKE and achieves the bandwidth rate $\frac{\lambda}{\mathsf{poly}(\lambda)}$. The public key, secret key, double key and ciphertext are very large in size since they contain a $O(\mathsf{poly}(\lambda))$ number of elements.
- The constructions of [12] from Goldwasser-Micali, Paillier, ElGamal and OAEP are instantiated using an additional generic symmetric key encryption scheme prE with pseudo-random ciphertext. Their bandwidth rate depends on the plaintext space of the underlying scheme (it exceeds 1 for Goldwasser-Micali). Moreover, they are not robust and the key-deniability property is not claimed. Our Π_{aGM} has $\alpha = 1$ whereas Π_{aBen} has $\alpha \gg 1$, both needs only a PRF and are robust and key-deniable. However, the covert rate is low in Π_{aGM} and for that reason the block variant Π_{aGMb} is the one to compare on covert bits per ciphertext bit.
- The ElGamal, Cramer-Shoup and OAEP-based AEs of [3] are robust, deniable and synchronized, like ours. They require the discrete logarithm problem to be hard in the plaintext space but easy in the covert plaintext space, hence the covert plaintext is tiny ($\varrho \leq 0.031$ for 16 covert bits and a 256-bit group element). Their double key is a PRF key plus a small term, which is comparable to our ν-bit key. The advantage of our schemes is the higher covert rate.
- The anamorphic constructions of [7] based on the Cramer-Shoup and GSW cryptosystem and the constructions of [14] based on ElGamal and Dual-Regev cryptosystems are *asymmetric*: a single anamorphic public key serves many senders, which is a real advantage over our symmetric double key. In exchange the receiver has to generate the anamorphic key together with a new key pair, which is suspicious to the dictator and gives no key deniability.

Table 2 Structural comparison of anamorphic PKE schemes

Scheme	Building Blocks	State	$\lvert\mathsf{dk}\rvert$ (secret part)	Deniability	Robustness	Assumption
Π_{RS} [1]	Rejection Sampling, PRF	L	-	×	×	secure PRF
Π_{NIZK} [1]	NIZK, NYT	L	-	×	×	secure PRF
Π_{aKW} [9]	hPRF, Π_{PKE}, $\mathcal{S}$	L	$\Omega(n\lvert K\rvert)$	×	×	secure hPRF, CCA aKW
Π_{aGM}, Π_{aPai}, Π_{aOAEP} [12]	prE	L	$\lvert K_{\mathsf{prE}}\rvert$	×	×	secure prE
Π_{aElG} [12]	prE	L	$\Theta(\lambda) + \lvert K_{\mathsf{prE}}\rvert$	×	×	secure prE
Π_{aElG}, Π_{aCS}, Π_{aOAEP} [3]	SRR PKE, PRF	S	$\lvert K\rvert + \Theta(l\lvert\mathbb{H}\rvert)$	✓	✓	PRF, DLP
Π_{aCS} [7]	HE/IBE-to-CCA	L	$8\lvert\mathbb{H}\rvert$	×	×	DLP
Π_{aGSW} [7]	HE/IBE-to-CCA	L	$vs\log_2 q$	×	×	LWE
Π_{aElG} [14]	PKE	L	$\lvert\mathbb{H}\rvert$	×	×	PRF, DLP
Π_{aDReg} [14]	PKE	L	$v\log_2 q$	×	×	LWE
Our Π_{aGM}	PRF	S	ν	✓	✓	QRP, PRF
Our Π_{aGMb}	PRF	S	ν	✓	✓	QRP, PRF
Our Π_{aBen}	PRF	S	ν	✓	✓	rRP, PRF
Our Π_{aPai}	PRF	S	ν	✓	✓	DCRA, PRF

S: synchronized (counter), L: stateless. Π_{RS}: rejection sampling based AE, Π_{NIZK}: Naor-Yung/NIZK based AE, Π_{aKW}: Koppula-Waters based AE, Π_{aGM}: Goldwasser-Micali PKE based AE, Π_{aPai}: Paillier PKE based AE, Π_{aOAEP}: RSA OAEP-based AE, Π_{aElG}: ElGamal-based AE, Π_{aCS}: Cramer-Shoup PKE based AE, Π_{aGSW}: GSW-based AE, Π_{aDReg}: Dual Regev-based AE, Π_{aGMb}: block Goldwasser Micali-based AE, Π_{aBen}: Benaloh PKE-based AE, hPRF: hinting PRF, Π_{PKE}: generic CPA secure PKE, $\mathcal{S}$: one-time strongly unforgeable signature, prE: symmetric encryption with pseudorandom ciphertexts, K: key of the PRF in [3], K_{prE}: key of the prE, $\lvert\mathbb{H}\rvert$: size of an element of the group $\mathbb{H}$, l: size of the covert plaintext space in [3], q, v: LWE parameters, $s = \lfloor\log_2 q\rfloor + 1$, ν: PRF key length for our constructions, QRP, rRP, DCRA: quadratic, r-th and decisional composite residuosity.

- *Symmetric versus asymmetric.* Our double key is shared per sender-receiver pair, so a receiver with many senders needs one double key and counter per sender. This is the price of key deniability and of generating the key from pk alone; it is a design trade-off and an application with many senders and no deniability requirement is better served by an asymmetric scheme.

2 Background

Definition 1 (Negligible function) [9] A function $\mu : \mathbb{N} \to \mathbb{R}^+$ is called negligible if $\forall c \geq 0$, $\exists N \in \mathbb{N}$ such that $\forall n \geq N$, $\mu(n) \leq n^{-c}$ where $\mathbb{R}^+$ is the set of all positive real numbers.

Definition 2 (PKE) [3]A PKE $\Pi_{\mathsf{PKE}} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, associated with plaintext space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ consisting of four *probabilistic polynomial time* (PPT) algorithms works as follows

$\mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda)$: The setup algorithm, run by some trusted central body at the beginning to set the public parameters, takes as input the security parameter λ and publishes the pp.

$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}(\mathsf{pp})$: A user runs the key generation algorithm on input pp to generate its secret key sk and public key pk, publishes pk and keeps sk secret.

$\mathsf{ct} \leftarrow \mathsf{Enc}(\mathsf{pp}, \mathsf{M}, \mathsf{pk})$: The sender runs the encryption algorithm with input the parameter pp, a plaintext $\mathsf{M} \in \mathcal{M}$ and the public key pk of the receiver, generates a ciphertext $\mathsf{ct} \in \mathcal{C}$ and sends it to the receiver. We refer ct generated by this algorithm as a normal ciphertext.

$\mathsf{M}' \leftarrow \mathsf{Dec}(\mathsf{pp}, \mathsf{ct}, \mathsf{sk})$: The receiver executes the decryption algorithm on input the parameter pp, a ciphertext ct and its own secret key sk and outputs a plaintext $\mathsf{M}' \in \mathcal{M}$.

Remark 1. Note that in spite of using a number of public parameters, most of the existing PKE schemes do not explicitly mention the public parameters. We consider a separate setup algorithm to generate and fix those parameters which creates clarity for practical implementation.

Definition 3 (Correctness) A PKE $\Pi_{\mathsf{PKE}} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is called correct if $\forall \lambda \in \mathbb{N}$ where $\mathbb{N}$ denotes the set of all natural numbers and all plaintext $\mathsf{M} \in \mathcal{M}$,

$$\Pr\left[\mathsf{M}' = \mathsf{M} \,\middle|\, \begin{array}{l} \mathsf{pp} \leftarrow \Pi_{\mathsf{PKE}}.\mathsf{Setup}(1^\lambda), (\mathsf{sk}, \mathsf{pk}) \leftarrow \Pi_{\mathsf{PKE}}.\mathsf{Gen}(\mathsf{pp}), \\ \mathsf{ct} \leftarrow \Pi_{\mathsf{PKE}}.\mathsf{Enc}(\mathsf{pp}, \mathsf{M}, \mathsf{pk}), \mathsf{M}' \leftarrow \Pi_{\mathsf{PKE}}.\mathsf{Dec}(\mathsf{pp}, \mathsf{ct}, \mathsf{sk}) \end{array}\right] = 1$$

Definition 4 (IND-CPA security) [9] A PKE Π_{PKE} is called IND-CPA secure if for all PPT adversary $\mathcal{A}$ and any $\lambda \in \mathbb{N}$, a negligible function $\mathsf{neg}(\cdot)$ exists such that

$$\mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\Pi_{\mathsf{PKE}},\mathcal{A}}(\lambda) = \left|\Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}CPA}}_{\Pi_{\mathsf{PKE}},\mathcal{A}}(\lambda) = 1\right] - \tfrac{1}{2}\right| < \mathsf{neg}(\lambda)$$

where the security experiment $\mathsf{Exp}^{\mathsf{IND\text{-}CPA}}_{\Pi_{\mathsf{PKE}},\mathcal{A}}(\lambda)$ run between the adversary $\mathcal{A}$ and a challenger $\mathbf{C}$, is depicted in Fig. 2.

Definition 5 (AE (Synchronous)) [3] For a PKE $\Pi_{\mathsf{PKE}} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with corresponding plaintext space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ (Def. 2), its synchronous AE

Table 3 Sizes and rates of anamorphic PKE schemes (symbolic; $\gamma = \beta/\alpha = |\mathsf{ct}|/|\widehat{\mathsf{M}}|$)

Scheme	Type	$\lvert\mathsf{pk}\rvert$	$\lvert\mathsf{sk}\rvert$	$\lvert\mathsf{dk}\rvert$	$\lvert\mathsf{ct}\rvert$	$\alpha = \frac{\lvert\widehat{\mathsf{M}}\rvert}{\lvert\mathsf{M}\rvert}$	$\beta = \frac{\lvert\mathsf{ct}\rvert}{\lvert\mathsf{M}\rvert}$	$\gamma = \frac{\lvert\mathsf{ct}\rvert}{\lvert\widehat{\mathsf{M}}\rvert}$	Assumption
Π_{saE} [3]	AExt	$\lvert\mathbb{H}\rvert$	$\lvert\mathbb{H}\rvert$	$\lvert K\rvert + \Theta(l(\lvert\mathbb{H}\rvert))$	$2\lvert\mathbb{H}\rvert$	$\frac{\log_2(\lvert\mathbb{H}\rvert)}{2\lvert\mathbb{H}\rvert}$	2	$\frac{4\lvert\mathbb{H}\rvert}{\log_2\lvert\mathbb{H}\rvert}$	PRF, DLP
Π_{saCS} [3]	AExt	$3\lvert\mathbb{H}\rvert$	$5\lvert\mathbb{H}\rvert$	$\lvert K\rvert + \Theta(l(\lvert\mathbb{H}\rvert))$	$4\lvert\mathbb{H}\rvert$	$\frac{\log_2(\lvert\mathbb{H}\rvert)}{4\lvert\mathbb{H}\rvert}$	4	$\frac{16\lvert\mathbb{H}\rvert}{\log_2\lvert\mathbb{H}\rvert}$	PRF, DLP
Π_{aCS} [7]	AEnc	$4\lvert\mathbb{H}\rvert$	$3\lvert\mathbb{H}\rvert$	$8\lvert\mathbb{H}\rvert$	$4\lvert\mathbb{H}\rvert$	$\frac{\log_2(\lvert\mathbb{H}\rvert)}{\lvert\mathbb{H}\rvert}$	4	$\frac{4\lvert\mathbb{H}\rvert}{\log_2\lvert\mathbb{H}\rvert}$	DLP
Π_{aGSW} [7]	AEnc	$mv\log_2 q$	$vs\log_2 q$	$vs\log_2 q$	U^2	1	mv	mv	LWE
Π_{aElG}[14]	AEnc	$\lvert\mathbb{H}\rvert$	$\lvert\mathbb{H}\rvert$	$\lvert\mathbb{H}\rvert$	$2\lvert\mathbb{H}\rvert$	$\frac{\log_2(\lvert\mathbb{H}\rvert)}{4\lvert\mathbb{H}\rvert}$	2	$\frac{8\lvert\mathbb{H}\rvert}{\log_2\lvert\mathbb{H}\rvert}$	PRF,DLP
Π_{aDReg}[14]	AEnc	$mv\log_2 q$	$v\log_2 q$	$v\log_2 q$	$(v+1)\log_2 q$	1	$(v+1)\log_2 q$	$(v+1)\log_2 q$	LWE
Π_{aBG}[13]	AExt	$\log_2 N$	$\log_2 N$	$2\log_2 N$	$n + \log_2 N$	$\frac{\sqrt{N}}{n}$	$\frac{n+\log_2 N}{n}$	$\frac{n+\log_2 N}{\sqrt{N}}$	QRP, PRF
Our Π_{aGM}	AExt	$2\log_2 N$	$\log_2 N$	ν	$n\log_2 N$	1	$\log_2 N$	$\log_2 N$	QRP, PRF
Our Π_{aGMb} (n elts)	AExt	$2\log_2 N$	$\log_2 N$	ν	$n\log_2 N$	ℓ	$\log_2 N$	$\frac{\log_2 N}{\ell}$	QRP, PRF
Our Π_{aBen}	AExt	$2\log_2 N$	$2\log_2 N$	ν	$\log_2 N$	$\frac{\ell}{\log_2 r}$	$\frac{\log_2 N}{\log_2 r}$	$\frac{\log_2 N}{\ell}$	rRP, PRF
Our Π_{aPai}	AExt	$\log_2 N$	$\log_2 N$	ν	$2\log_2 N$	≈ 1	2	$\frac{2\log_2 N}{\ell_P}$	DCRA, PRF

AExt: anamorphic extension, AEnc: anamorphic encryption, $|\mathbb{H}|$: size of an element of the group $\mathbb{H}$, $|K|$: PRF key in the double key of [3], l: size of the covert plaintext space in [3], q, v, m: LWE parameters, $s = \lfloor \log_2 q \rfloor + 1$, $U = vs$, N: modulus, n: plaintext size in Π_{aGM}, Π_{aGMb}, Π_{aBG}, $\ell = \lambda - 2 - \tau$ and $\ell_P = 2\lambda - 3 - \tau$: covert payload bits per element (τ: redundancy bits, $\lambda = \log_2 N/2$), ν: PRF key length (secret part of dk; pk is public and not counted), α: bandwidth rate, β: ciphertext expansion rate, γ: anamorphic ciphertext expansion rate. For the schemes of other authors the $|\cdot|$, $\Pi_{\mathsf{saE}}, \Pi_{\mathsf{saCS}}$: synchronized AEs of ElGamal and Cramer-Shoup [3]; $\Pi_{\mathsf{aCS}}, \Pi_{\mathsf{aGSW}}$ $\Pi_{\mathsf{aElG}}, \Pi_{\mathsf{aDReg}}$: AEs from Cramer-Shoup PKE, GSW cryptosystem [7], Elgamal and dual Regev PKE [14].

Table 4 Concrete sizes at the 128-bit security level ($|N| = 3072$, $r = 65537$, $\tau = \nu = 128$; bits)

Scheme	$\lvert\mathsf{pk}\rvert$	$\lvert\mathsf{sk}\rvert$	$\lvert\mathsf{dk}\rvert$	$\lvert\mathsf{ct}\rvert$	$\lvert\widehat{\mathsf{M}}\rvert$	ϱ
Π_{aGM} ($n = 128$)	6144	3072	128	393216	128	0.0003
Π_{aGMb} ($n = 8$)	6144	3072	128	24576	11248	0.458
Π_{aBen}	6144	6144	128	3072	1406	0.458
Π_{aPai}	3072	3072	128	6144	2941	0.479
ElGamal AE, FFC 3072/256, $b = 16$	3072	256	128	6144	16	0.0026
ElGamal AE, EC 256-bit, $b = 16$ (analytic)	256	256	128	512	16	0.031

The ElGamal rows follow the PRF-shifted-randomness technique of [3] with a b-bit covert space recovered by a discrete-logarithm table; $b \leq 40$ is the practical limit, so even at $b = 40$ the EC variant reaches $\varrho < 0.08$. The Π_{aBen} secret key is stored as (p, q, x) with $|x| = \log_2 N$. 128-bit PRF keys for all schemes.

$\mathsf{Exp}^{\mathsf{IND\text{-}CPA}}_{\Pi_{\mathsf{PKE}},\mathcal{A}}(\lambda)$

Setup phase. The challenger $\mathbf{C}$ runs $\Pi_{\mathsf{PKE}}.\mathsf{Setup}(\lambda)$ for generating public parameters pp and then computes a key pair $(\mathsf{sk}, \mathsf{pk}) \leftarrow \Pi_{\mathsf{PKE}}.\mathsf{Gen}(\mathsf{pp})$. It provides $(\mathsf{pp}, \mathsf{pk})$ to the adversary $\mathcal{A}$ while keeping sk secret.

Challenge phase. Upon receiving a challenge plaintext pair (m_0^*, m_1^*) from $\mathcal{A}$, the challenger samples a bit $b \xleftarrow{\$} \{0, 1\}$ and computes the ciphertext $\mathsf{ct}^* \leftarrow \Pi_{\mathsf{PKE}}.\mathsf{Enc}(\mathsf{pp}, \mathsf{pk}, m_b^*)$ and sends it to $\mathcal{A}$.

Guess phase. Finally, the adversary $\mathcal{A}$ outputs a guess bit b'. The challenger returns 1 as the output of the experiment $\mathsf{Exp}^{\mathsf{IND\text{-}CPA}}_{\Pi_{\mathsf{PKE}},\mathcal{A}}(\lambda)$ if $b' = b$ and 0 otherwise.

Fig. 2 $\mathsf{Exp}^{\mathsf{IND\text{-}CPA}}_{\Pi_{\mathsf{PKE}},\mathcal{A}}(\lambda)$: Indistinguishability against CPA

$\Pi_{\mathsf{aPKE}} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ associated with the covert plaintext space $\widehat{\mathcal{M}}$, consists of the following four additional PPT algorithms.

$\mathsf{ap} \leftarrow \mathsf{Setup}(\mathsf{pk})$: The anamorphic setup algorithm, which can be run by any party (the sender, the receiver or a trusted authority) because it uses only public input, takes as input the public key pk of the receiver and publishes an anamorphic public parameter ap.
Here $(\mathsf{sk}, \mathsf{pk}) \leftarrow \Pi_{\mathsf{PKE}}.\mathsf{Gen}(\mathsf{pp})$ is the secret-public key pair of the receiver who has kept sk secret to itself and made pk publicly available and $\mathsf{pp} \leftarrow \Pi_{\mathsf{PKE}}.\mathsf{Setup}(1^\lambda)$ is the public parameter generated on input the security parameter λ at the beginning.

$(\mathsf{dk}, \mathsf{ctr}) \leftarrow \mathsf{Gen}(\mathsf{ap}, \mathsf{pk})$: The anamorphic key generation algorithm enables a user to generate a double key dk and a counter ctr on input the anamorphic parameter ap and a public key pk of a receiver. This algorithm can be run by the sender (or receiver) who sends the pair $(\mathsf{dk}, \mathsf{ctr})$ to the receiver (or sender) securely.

$(\mathsf{ct}, \mathsf{ctr}) \leftarrow \mathsf{Enc}(\mathsf{ap}, \mathsf{M}, \widehat{\mathsf{M}}, \mathsf{dk}, \mathsf{ctr})$: The anamorphic encryption algorithm is executed by a sender who on input the anamorphic parameter ap, a plaintext $\mathsf{M} \in \mathcal{M}$, a covert plaintext $\widehat{\mathsf{M}} \in \widehat{\mathcal{M}}$, a double key dk and a counter ctr, outputs a ciphertext $\mathsf{ct} \in \mathcal{C}$ and an updated counter ctr. We refer ct generated by this algorithm as anamorphic ciphertext.

$(\widehat{\Gamma}/\perp, \mathsf{ctr}) \leftarrow \mathsf{Dec}(\mathsf{ap}, \mathsf{ct}, \mathsf{sk}, \mathsf{dk}, \mathsf{ctr})$: The decryption algorithm is run by the receiver who takes as input the anamorphic parameter ap, a ciphertext $\mathsf{ct} \in \mathcal{C}$, its secret key sk, double key

dk and a counter ctr and produces either $\widehat{\Gamma} \in \widehat{\mathcal{M}}$ or a special symbol $\perp$ (decryption failure) and an updated counter ctr.

Remark 2. Note that the counter ctr is initialized once in the beginning and gets updated by the encryptor (resp. the decryptor) after each anamorphic encryption (resp. anamorphic decryption). More specifically, at any point of time the encryptor and the decryptor hold the same counter. The anamorphic parameter and the double key are generated using only the public key of the receiver which ensures that the receiver has the full potential to deny the ownership ap and dk.
Though the existing AE schemes do not specifically mention any anamorphic public parameter ap, all of them use some common parameters. Therefore, in our definition we intend to formalize those parameters and generate through a proper setup algorithm.

Definition 6 (Correctness) (overwhelming; the PRF-based schemes below can fail only when two pseudo-random values collide) An AE $\Pi_{\mathsf{aPKE}} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ of a PKE $\Pi_{\mathsf{PKE}} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is defined to be correct if $\forall \lambda \in \mathbb{N}$, all plaintext $\mathsf{M} \in \mathcal{M}$ and all covert plaintext $\widehat{\mathsf{M}} \in \widehat{\mathcal{M}}$,

$$\Pr\left[\begin{array}{l|l} \widehat{\Gamma} = \widehat{\mathsf{M}} & \mathsf{pp} \leftarrow \Pi_{\mathsf{PKE}}.\mathsf{Setup}(1^\lambda), (\mathsf{sk}, \mathsf{pk}) \leftarrow \Pi_{\mathsf{PKE}}.\mathsf{Gen}(\mathsf{pp}), \\ \mathsf{M}' = \mathsf{M} & \mathsf{ap} \leftarrow \Pi_{\mathsf{aPKE}}.\mathsf{Setup}(\mathsf{pk}), (\mathsf{dk}, \mathsf{ctr}) \leftarrow \Pi_{\mathsf{aPKE}}.\mathsf{Gen}(\mathsf{ap}, \mathsf{pk}), \\ & (\mathsf{ct}, \mathsf{ctr}) \leftarrow \Pi_{\mathsf{aPKE}}.\mathsf{Enc}(\mathsf{ap}, \mathsf{M}, \widehat{\mathsf{M}}, \mathsf{dk}, \mathsf{ctr}), \\ & \mathsf{M}' \leftarrow \Pi_{\mathsf{PKE}}.\mathsf{Dec}(\mathsf{pp}, \mathsf{ct}, \mathsf{sk}), \\ & (\widehat{\Gamma}, \mathsf{ctr}) \leftarrow \Pi_{\mathsf{aPKE}}.\mathsf{Dec}(\mathsf{ap}, \mathsf{ct}, \mathsf{sk}, \mathsf{dk}, \mathsf{ctr}) \end{array}\right] \geq 1 - \mathsf{neg}(\lambda)$$

Definition 7 (Computational robustness) An AE $\Pi_{\mathsf{aPKE}} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ of a PKE $\Pi_{\mathsf{PKE}} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is defined to be computationally robust if $\forall \lambda \in \mathbb{N}$, a negligible function $\mathsf{neg}(\cdot)$ exists so that for all plaintext $\mathsf{M} \in \mathcal{M}$,

$$\Pr\left[\widehat{\Gamma} \neq \perp \left| \begin{array}{l} \mathsf{pp} \leftarrow \Pi_{\mathsf{PKE}}.\mathsf{Setup}(1^\lambda), (\mathsf{sk}, \mathsf{pk}) \leftarrow \Pi_{\mathsf{PKE}}.\mathsf{Gen}(\mathsf{pp}), \\ \mathsf{ap} \leftarrow \Pi_{\mathsf{aPKE}}.\mathsf{Setup}(\mathsf{pk}), (\mathsf{dk}, \mathsf{ctr}) \leftarrow \Pi_{\mathsf{aPKE}}.\mathsf{Gen}(\mathsf{ap}, \mathsf{pk}), \\ \mathsf{ct} \leftarrow \Pi_{\mathsf{PKE}}.\mathsf{Enc}(\mathsf{pp}, \mathsf{M}, \mathsf{pk}) \\ (\widehat{\Gamma}, \mathsf{ctr}) \leftarrow \Pi_{\mathsf{aPKE}}.\mathsf{Dec}(\mathsf{ap}, \mathsf{ct}, \mathsf{sk}, \mathsf{dk}, \mathsf{ctr}) \end{array}\right.\right] < \mathsf{neg}(\lambda)$$

i.e., a normal ciphertext can be anamorphically decrypted only with negligible probability.

Definition 8 (IND-NA security) [3] An AE $\Pi_{\mathsf{aPKE}} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ of a PKE $\Pi_{\mathsf{PKE}} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is called IND-NA secure if $\forall \lambda \in \mathbb{N}$ and all PPT distinguisher $\mathcal{D}$, a negligible function $\mathsf{neg}(\cdot)$ exists such that

$$\mathsf{Adv}^{\mathsf{IND\text{-}NA}}_{\Pi_{\mathsf{aPKE}}, \mathcal{D}}(\lambda) = \left| \Pr\left[\mathsf{Exp}^{\mathsf{IND\text{-}NA}}_{\Pi_{\mathsf{aPKE}}, \mathcal{D}}(\lambda) = 1\right] - \frac{1}{2} \right| < \mathsf{neg}(\lambda)$$

where the experiment $\mathsf{Exp}^{\mathsf{IND\text{-}NA}}_{\Pi_{\mathsf{aPKE}}, \mathcal{D}}(\lambda)$ between the distinguisher $\mathcal{D}$ and a challenger $\mathbf{C}$ is presented in Fig. 3.

Definition 9 (Quadratic residue (QR)) [15] An integer a with $\gcd(a, N) = 1$ where $N > 0$, is called a QR modulo N if $x^2 = a \bmod N$ for some integer x.

$\underline{\mathsf{Exp}^{\mathsf{IND\text{-}NA}}_{\Pi_{\mathsf{aPKE}},\mathcal{D}}(\lambda)}$

Setup phase. The challenger $\mathbf{C}$ produces the public parameter $\mathsf{pp} \leftarrow \Pi_{\mathsf{PKE}}.\mathsf{Setup}(1^\lambda)$, the key pair $(\mathsf{sk}, \mathsf{pk}) \leftarrow \Pi_{\mathsf{PKE}}.\mathsf{Gen}(\mathsf{pp})$, the anamorphic parameter $\mathsf{ap} \leftarrow \Pi_{\mathsf{aPKE}}.\mathsf{Setup}(\mathsf{pk})$, the double key and counter pair $(\mathsf{dk}, \mathsf{ctr}) \leftarrow \Pi_{\mathsf{aPKE}}.\mathsf{Gen}(\mathsf{ap}, \mathsf{pk})$ and returns $(\mathsf{pp}, \mathsf{sk}, \mathsf{pk})$ to the distinguisher $\mathcal{D}$.

Challenge phase. The challenger $\mathbf{C}$ samples $b \xleftarrow{\$} \{0,1\}$ and provides the $\mathcal{D}$ the encryption oracle $\mathcal{O}^b_{\mathsf{Enc}}(\cdot,\cdot)$ where $\mathcal{O}^0_{\mathsf{Enc}}(\cdot,\cdot)$ is the normal encryption oracle and $\mathcal{O}^1_{\mathsf{Enc}}(\cdot,\cdot)$ is the anamorphic encryption oracle which respond as follows to the queries of the form $(\mathsf{M}, \widehat{\mathsf{M}}) \in \mathcal{M} \times \widehat{\mathcal{M}}$ made by $\mathcal{D}$.

$$\mathcal{O}^0_{\mathsf{Enc}}(\mathsf{M}, \widehat{\mathsf{M}}) \rightarrow \mathsf{ct} \text{ where } \mathsf{ct} \leftarrow \Pi_{\mathsf{PKE}}.\mathsf{Enc}(\mathsf{pp}, \mathsf{M}, \mathsf{pk})$$
$$\mathcal{O}^1_{\mathsf{Enc}}(\mathsf{M}, \widehat{\mathsf{M}}) \rightarrow \mathsf{ct} \text{ where } (\mathsf{ct}, \mathsf{ctr}) \leftarrow \Pi_{\mathsf{aPKE}}.\mathsf{Enc}(\mathsf{ap}, \mathsf{M}, \widehat{\mathsf{M}}, \mathsf{dk}, \mathsf{ctr})$$

Query phase. The distinguisher $\mathcal{D}$ can query to $\mathcal{O}^b_{\mathsf{Enc}}(\cdot,\cdot)$ polynomially many times.

Guess phase. The distinguisher $\mathcal{D}$ returns to $\mathbf{C}$ a bit b' as a guess for the bit b. Finally, $\mathbf{C}$ returns 1 as the output of the game $\mathsf{Exp}^{\mathsf{IND\text{-}NA}}_{\Pi_{\mathsf{aPKE}},\mathcal{D}}(\lambda)$ when $b = b'$ and 0 otherwise.

Fig. 3 $\mathsf{Exp}^{\mathsf{IND\text{-}NA}}_{\Pi_{\mathsf{aPKE}},\mathcal{D}}(\lambda)$: IND-NA Security experiment

The set of all QRs modulo N is denoted by $\mathsf{QR}(N)$.

Definition 10 (PQR) [15] Let $N > 0$ and a are integers with $\gcd(a, N) = 1$. Then a is called a PQR modulo N if $\left(\frac{a}{N}\right) = 1$ and $\nexists x$ such that $x^2 = a \bmod N$ where $\left(\frac{a}{N}\right)$ denotes the Legendre symbol of the integer a modulo N.

The set of all PQRs modulo N is denoted by $\mathsf{PQR}(N)$.

Definition 11 (Secure PRF) [3] A PRF $F : \mathcal{K} \times \mathcal{X} \rightarrow \mathcal{Y}$ is said to be secure if, for a uniformly random key $K \in \mathcal{K}$, the function $F(K, \cdot)$ is indistinguishable from a function $f : \mathcal{X} \rightarrow \mathcal{Y}$ chosen uniformly from the collection $\mathcal{F}^{\mathcal{Y}}_{\mathcal{X}}$ of all functions from $\mathcal{X}$ to $\mathcal{Y}$. More specifically, $\forall \lambda \in \mathbb{N}$ and every PPT distinguisher $\mathcal{D}$, a negligible function $\mathsf{neg}(\cdot)$ exists such that

$$\mathsf{Adv}^{\mathsf{PRF}}_{F,\mathcal{D}}(\lambda) = \left|\Pr\left[\mathcal{D}^{F(K,\cdot)}(\lambda) = 1\right] - \Pr\left[\mathcal{D}^{f(\cdot)}(\lambda) = 1\right]\right| < \mathsf{neg}(\lambda)$$

Equivalently, $|\Pr[\mathsf{Exp}^{\mathsf{IND\text{-}PRF}}_{F,\mathcal{D}}(\lambda) = 1] - \frac{1}{2}| = \frac{1}{2}\mathsf{Adv}^{\mathsf{PRF}}_{F,\mathcal{D}}(\lambda)$ for the experiment $\mathsf{Exp}^{\mathsf{IND\text{-}PRF}}_{F,\mathcal{D}}(\lambda)$ between $\mathcal{D}$ and a challenger $\mathbf{C}$ in Fig. 4 for $b \in \{0,1\}$. We denote $\mathsf{Adv}^{\mathsf{PRF}}_{F,\mathcal{D}}(\lambda)$ by $\mathsf{Adv}^{\mathsf{PRF}}_{F}(\lambda)$ when there is no ambiguity. The advantage is written without the factor $\frac{1}{2}$ so that the reductions below can be stated as $|\Pr[E_i] - \Pr[E_{i+1}]| \leq \mathsf{Adv}^{\mathsf{PRF}}_{F}(\lambda)$.

Parameters and PRF instantiation.

Throughout, λ is the bit length of each of the two primes of $N = pq$ (so $2^{2\lambda-2} < N < 2^{2\lambda}$ and $|N| \approx 2\lambda$; for 128-bit security $|N| = 3072$ and $\lambda = 1536$), ν is the length of a PRF key ($\nu = 128$), ξ is a statistical slack parameter ($\xi = 128$), τ is the length of a

$\underline{\mathsf{Exp}^{\mathsf{IND\text{-}PRF}}_{F,\mathcal{D}}(\lambda)}$

Setup phase. The challenger $\mathbf{C}$ samples a key $K \xleftarrow{\$} \mathcal{K}$ and a uniformly random function $f : \mathcal{X} \to \mathcal{Y}$ from the collection $\mathcal{F}^{\mathcal{Y}}_{\mathcal{X}}$ of all functions from $\mathcal{X}$ to $\mathcal{Y}$ i.e., $f \xleftarrow{\$} \mathcal{F}^{\mathcal{Y}}_{\mathcal{X}}$.

Challenge phase. The challenger $\mathbf{C}$ samples $b \xleftarrow{\$} \{0,1\}$ and gives $\mathcal{D}$ the access to the PRF oracle $\mathcal{O}^b_{\mathsf{PRF}}(\cdot)$ where $\mathcal{O}^0_{\mathsf{PRF}}(\cdot)$ and $\mathcal{O}^1_{\mathsf{PRF}}(\cdot)$ respond as follows to the query on $x \in \mathcal{X}$

$$\mathcal{O}^0_{\mathsf{PRF}}(x) \to F(K,x)$$
$$\mathcal{O}^1_{\mathsf{PRF}}(x) \to f(x)$$

Query phase. The distinguisher $\mathcal{D}$ can query to the oracle $\mathcal{O}^b_{\mathsf{PRF}}(\cdot)$ polynomially many times.

Guess phase. The distinguisher returns to $\mathbf{C}$ a bit b' as a guess for the bit b chosen by $\mathbf{C}$.

Fig. 4 $\mathsf{Exp}^{\mathsf{IND\text{-}PRF}}_{F,\mathcal{D}}$: Indistinguishability security experiment for PRF $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$

redundancy tag and $T = 2^{64}$ is the size of the counter space. All asymptotic statements are in terms of λ. For a modulus N let $\psi_N : \{0,1\}^{2\lambda+\xi} \to \mathbb{Z}^*_N$ map s to $s \bmod N$ if this is coprime to N and to 1 otherwise. Given a PRF $G : \{0,1\}^\nu \times \{0,1\}^* \to \{0,1\}^{2\lambda+\xi}$ (for instance HMAC-SHA-256 in counter mode) we use $F = \psi_N \circ G : \{0,1\}^\nu \times \{0,1\}^* \to \mathbb{Z}^*_N$ as a PRF with range $\mathbb{Z}^*_N$.
For a homomorphism σ_e over $\mathbb{Z}^*_N$ with $\sigma_e(u) = u^e$ maps onto its image $\Delta_e = \{u^e \mid u \in \mathbb{Z}^*_N\}$. We use $F^{(e)} = \sigma_e \circ F : \{0,1\}^\nu \times \{0,1\}^* \to \Delta_e$ as a PRF with range Δ_e. We take $e = 2$ for the Goldwasser-Micali-based AEs, $e = r$ for the Benaloh PKE-based construction, $e = N^s$ for the Damgård-Jurik AE and $e = N$ for the Paillier AE.

Lemma 1. For every adversary $\mathcal{A}$ for PRF F that makes at most q queries to its oracle, there is a PRF adversary $\mathcal{A}'$ against G with the same running time and up to $O(q)$ evaluations of ψ_N such that

$$\mathsf{Adv}^{\mathsf{PRF}}_{F,\mathcal{A}}(\lambda) \le \mathsf{Adv}^{\mathsf{PRF}}_{G,\mathcal{A}'}(\lambda) + q\,(2^{-\xi} + 2^{-\lambda+2})$$

where F, G, ψ_N are as described above. The same bound holds for $F^{(e)}$ against a uniformly random function into Δ_e.

Proof The PRF challenger $\mathbf{C}$ for the PRF $G : \{0,1\}^\nu \times \{0,1\}^* \to \{0,1\}^{2\lambda+\xi}$, samples a uniformly random function R and chooses a key $K \xleftarrow{\$} \{0,1\}^\nu$. Then $\mathbf{C}$ chooses $b \xleftarrow{\$} \{0,1\}$ and provides $\mathcal{A}'$ oracle access to $G(K,\cdot)$ if $b = 0$ and $R(\cdot)$ if $b = 1$. Then $\mathcal{A}'$ uses the PRF adversary $\mathcal{A}$ for the PRF F as follows. It applies ψ_N to the received challenge oracle and sends to $\mathcal{A}$. Clearly, $\mathcal{A}$ gets the oracle for $\psi_N \circ G(K,\cdot) = F(K,\cdot)$ if $b = 0$ and $\psi_N \circ R(\cdot)$ if $b = 1$. Therefore,

$$\left|\Pr[\mathcal{A}^{F(K,\cdot)} = 1] - \Pr[\mathcal{A}^{\psi_N \circ R(\cdot)} = 1]\right| = \mathsf{Adv}^{\mathsf{PRF}}_{G,\mathcal{A}'}(\lambda)$$

For distinct inputs R returns independent uniform strings of $2\lambda + \xi$ bits. A uniform string reduced modulo N is within statistical distance $N/2^{2\lambda+\xi} \le 2^{-\xi}$ of the uniform distribution on $\mathbb{Z}_N$. A uniform element of $\mathbb{Z}_N$ is outside $\mathbb{Z}^*_N$ with probability $\frac{p+q-1}{pq} < 2^{-\lambda+2}$ because

$p, q > 2^{\lambda-1}$ and conditioned on being a unit it is uniform on $\mathbb{Z}_N^*$. Hence, each output of $\psi_N \circ R$ is within distance $2^{-\xi} + 2^{-\lambda+2}$ of uniform on $\mathbb{Z}_N^*$.
The outputs for distinct inputs are independent and repeated inputs repeat in both worlds; the claim follows by a union bound over at most q distinct inputs. Therefore, if $f : \{0,1\}^* \to \mathbb{Z}_N^*$ be a uniformly random function,

$$\left|\Pr[\mathcal{A}^{\psi_N \circ R(\cdot)} = 1] - \Pr[\mathcal{A}^{f(\cdot)} = 1]\right| \leq q(2^{-\xi} + 2^{-\lambda+2})$$

Therefore,

$$\mathsf{Adv}^{\mathsf{PRF}}_{F,\mathcal{A}}(\lambda) = \left|\Pr[\mathcal{A}^{F(K,\cdot)} = 1] - \Pr[\mathcal{A}^{f(\cdot)} = 1]\right| \leq \mathsf{Adv}^{\mathsf{PRF}}_{G,\mathcal{A}'}(\lambda) + q(2^{-\xi} + 2^{-\lambda+2})$$

If $F : \{0,1\}^\nu \times \{0,1\}^* \to \mathbb{Z}_N^*$ is uniform on $\mathbb{Z}_N^*$ then $F^{(e)} = \sigma_e \circ F : \{0,1\}^\nu \times \{0,1\}^* \to \Delta_e$ is uniform on Δ_e because $\sigma_e : \mathbb{Z}_N^* \to \Delta_e$ with $\sigma_e(u) = u^e \bmod N$ is a surjective group homomorphism onto Δ_e whose fibres all have the same size. □

3 Our construction Π_{aGM}: synchronous AE from Goldwasser-Micali PKE

Consider the Goldwasser-Micali PKE Π_{GM} associated with the plaintext space $\mathcal{M} = \{0,1\}^n$ and the ciphertext space $\mathcal{C} = \mathbb{Z}_N^n$. We describe below its AE Π_{aGM} associated with the covert plaintext space $\widehat{\mathcal{M}} = \{0,1\}^n$ that uses the PRF $F = \psi_N \circ G : \{0,1\}^\nu \times (\mathbb{Z}_T \times [n] \times \{0,1\}) \to \mathbb{Z}_N^*$ of Lemma 1.

Initially, $\Pi_{\mathsf{GM}} = \begin{bmatrix} \mathsf{Setup}(\lambda) \to \mathsf{pp} \\ \mathsf{Gen}(\mathsf{pp}) \to (\mathsf{sk}, \mathsf{pk}) \\ \mathsf{Enc}(\mathsf{pp}, \mathsf{M}, \mathsf{pk}) \to \mathsf{ct} \\ \mathsf{Dec}(\mathsf{pp}, \mathsf{ct}, \mathsf{sk}) \to \mathsf{M} \end{bmatrix}$ is in active mode where the normal public parameter $\mathsf{pp} = \mathcal{G}_\lambda$ is generated by a trusted authority by using the algorithm $\Pi_{\mathsf{GM}}.\mathsf{Setup}$ where $\mathcal{G}_\lambda$ generates random λ-bit primes. A user runs the algorithm $\Pi_{\mathsf{GM}}.\mathsf{Gen}$ on input pp and generates its secret key $\mathsf{sk} = (p, q)$ and the corresponding public key $\mathsf{pk} = (N, x)$ where (p, q) is a pair of λ-bit primes generated by $\mathcal{G}_\lambda$, $N = pq$ and $x \in \mathsf{PQR}(N)$ is a PQR modulo N. The secret key is kept secret to the user itself whereas the public key is published. The sender runs the algorithm $\Pi_{\mathsf{GM}}.\mathsf{Enc}$ on input of the public parameter pp, a plaintext $\mathsf{M} \in \mathcal{M} = \{0,1\}^n$ and the public key pk of the receiver, generates a ciphertext $\mathsf{ct} = c_1 \dots c_n \in \mathcal{C} = \mathbb{Z}_N^n$ where $c_i = y_i^2 x^{m_i} \bmod N$ with $y_i \xleftarrow{\$} \mathbb{Z}_N^*$ and sends it to the receiver. The receiver runs the algorithm $\Pi_{\mathsf{GM}}.\mathsf{Dec}$ on input of the public parameter pp, a ciphertext $\mathsf{ct} = c_1 \dots c_n \in \mathbb{Z}_N^n$ and its secret key $\mathsf{sk} = (p, q)$ and recovers the plaintext $\mathsf{M}' = m'_1 \dots m'_n \in \{0,1\}^n$ where $m'_i = 0$ if c_i is a QR modulo p and q and $m'_i = 1$ otherwise.

The four PPT algorithms of the AE $\Pi_{\mathsf{aGM}} = \begin{bmatrix} \mathsf{Setup}(\mathsf{pk}) \to \mathsf{ap} \\ \mathsf{Gen}(\mathsf{ap}, \mathsf{pk}) \to (\mathsf{dk}, \mathsf{ctr}) \\ \mathsf{Enc}(\mathsf{ap}, \mathsf{M}, \widehat{\mathsf{M}}, \mathsf{dk}, \mathsf{ctr}) \to (\mathsf{ct}, \mathsf{ctr}) \\ \mathsf{Dec}(\mathsf{ap}, \mathsf{ct}, \mathsf{sk}, \mathsf{dk}, \mathsf{ctr}) \to (\widehat{\Gamma}, \mathsf{ctr}) \end{bmatrix}$ work as follows.

- The algorithm $\Pi_{\mathsf{aGM}}.\mathsf{Setup}$ described in Algorithm 1 may be run by any party (sender, receiver or an authority) because it only uses the public key $\mathsf{pk} = (N, x)$. It sets the anamorphic parameters ap, which are just the description of the PRF

$F = \psi_N \circ G : \{0,1\}^\nu \times (\mathbb{Z}_T \times [n] \times \{0,1\}) \to \mathbb{Z}_N^*$; no secret randomness is involved and $G : \{0,1\}^\nu \times (\mathbb{Z}_T \times [n] \times \{0,1\}) \to \{0,1\}^{2\lambda+\xi}$ can be a fixed public standard.

Algorithm 1 $\Pi_{\mathsf{aGM}}.\mathsf{Setup}(\mathsf{pk}) \to \mathsf{ap}$

1: $\mathsf{ap} = F = \psi_N \circ G$ with G a fixed public PRF;

- The algorithm $\Pi_{\mathsf{aGM}}.\mathsf{Gen}$ given in Algorithm 2 is run by the sender (resp. the receiver) with input ap and the public key $\mathsf{pk} = (N, x)$ of the receiver to generate a double key $\mathsf{dk} = (K, \mathsf{pk})$ and a counter ctr where $K \in \{0,1\}^\nu$ and $\mathsf{ctr} \in \mathbb{Z}_T$. The secret part of dk is the ν-bit key K. The pair is communicated to the receiver (resp. the sender) through a secure channel.

Algorithm 2 $\Pi_{\mathsf{aGM}}.\mathsf{Gen}(\mathsf{ap}, \mathsf{pk}) \to (\mathsf{dk}, \mathsf{ctr})$

1: $K \xleftarrow{\$} \{0,1\}^\nu$; $\mathsf{ctr} \xleftarrow{\$} \mathbb{Z}_T$;
2: $\mathsf{dk} = (K, \mathsf{pk})$;

- The algorithm $\Pi_{\mathsf{aGM}}.\mathsf{Enc}$ presented in Algorithm 3 is run by the sender on input ap, a normal plaintext $\mathsf{M} = m_1 \dots m_n \in \{0,1\}^n$, a covert plaintext $\widehat{\mathsf{M}} = \widehat{m}_1 \dots \widehat{m}_n \in \{0,1\}^n$, the double key dk and a counter ctr. It outputs $\mathsf{ct} = c_1 \dots c_n \in \mathbb{Z}_N^n$ and updates $\mathsf{ctr} = \mathsf{ctr} + 1 \bmod T$. The counter must be advanced and stored *before* the ciphertext leaves the sender (see Proposition 11).

Algorithm 3 $\Pi_{\mathsf{aGM}}.\mathsf{Enc}(\mathsf{ap}, \mathsf{M}, \widehat{\mathsf{M}}, \mathsf{dk}, \mathsf{ctr}) \to (\mathsf{ct}, \mathsf{ctr})$

1: **for** $(i = 1$ to $n)$ **do**
2: $\quad \beta_i = m_i \oplus \widehat{m}_i$;
3: $\quad y_i = F(K, (\mathsf{ctr}, i, \beta_i))$;
4: $\quad c_i = y_i^2 x^{m_i} \bmod N$;
5: **end for**
6: $\mathsf{ct} = c_1 \dots c_n$; $\mathsf{ctr} = \mathsf{ctr} + 1 \bmod T$;

- The algorithm $\Pi_{\mathsf{aGM}}.\mathsf{Dec}$ given in Algorithm 4 is run by the receiver on input ap, $\mathsf{ct} = c_1 \dots c_n \in \mathbb{Z}_N^n$, $\mathsf{sk} = (p, q)$, dk and ctr. It recovers $\widehat{\Gamma} \in \{0,1\}^n \cup \{\perp\}$ and the updated counter. One Legendre symbol computation and up to two PRF evaluations are needed per position and x^{-1} is computed once.

Theorem 2 *The AE Π_{aGM} is correct up to a negligible failure probability:* $\Pr[\widehat{\Gamma} \neq \widehat{\mathsf{M}}] \leq n\, 2^{-(2\lambda-4)}$. *Moreover, the normal decryption of an anamorphic ciphertext returns* M.

Algorithm 4 $\Pi_{\mathsf{aGM}}.\mathsf{Dec}(\mathsf{ap}, \mathsf{ct}, \mathsf{sk}, \mathsf{dk}, \mathsf{ctr}) \to (\widehat{\Gamma}, \mathsf{ctr})$

1: **for** $(i = 1$ to $n)$ **do**
2: **if** $\left(\left(\frac{c_i}{p}\right) = 1\right)$ **then**
3: $m_i = 0$; $z_i = c_i$;
4: **else**
5: $m_i = 1$; $z_i = c_i x^{-1} \bmod N$;
6: **end if**
7: **end for**
8: $\mathsf{M} = m_1 \dots m_n$; $\widehat{\Gamma} = \epsilon$;
9: **for** $(i = 1$ to $n)$ **do**
10: **if** $z_i = (F(K, (\mathsf{ctr}, i, 0)))^2 \bmod N$ **then**
11: $\widehat{\gamma}_i = m_i$;
12: **else if** $z_i = (F(K, (\mathsf{ctr}, i, 1)))^2 \bmod N$ **then**
13: $\widehat{\gamma}_i = 1 - m_i$;
14: **else**
15: $\widehat{\Gamma} = \perp$; **break**;
16: **end if**
17: **end for**
18: **if** $\widehat{\Gamma} \neq \perp$ **then**
19: $\widehat{\Gamma} = \widehat{\gamma}_1 \dots \widehat{\gamma}_n$;
20: **end if**
21: $\mathsf{ctr} = \mathsf{ctr} + 1 \bmod T$;

Proof Let

$$\begin{aligned}
&\mathsf{pp} = \mathcal{G}_\lambda \leftarrow \Pi_{\mathsf{GM}}.\mathsf{Setup}(1^\lambda)\\
&(\mathsf{sk} = (p, q), \mathsf{pk} = (N, x)) \leftarrow \Pi_{\mathsf{GM}}.\mathsf{Gen}(\mathsf{pp})\\
&\mathsf{ap} = F \leftarrow \Pi_{\mathsf{aGM}}.\mathsf{Setup}(\mathsf{pk})\\
&(\mathsf{dk} = (K, \mathsf{pk}), \mathsf{ctr}) \leftarrow \Pi_{\mathsf{aGM}}.\mathsf{Gen}(\mathsf{ap}, \mathsf{pk})
\end{aligned}$$

where λ is security parameter, $\mathcal{G}_\lambda$ is a λ-bit prime generator, p, q are two λ-bit primes generated by $\mathcal{G}_\lambda$, $N = pq$, $x \in \mathsf{PQR}(N)$ is a PQR modulo N, $F : \{0,1\}^\nu \times (\mathbb{Z}_T \times [n] \times \{0,1\}) \to \mathbb{Z}_N^*$ is a random PRF, $K \in \{0,1\}^\nu$ and $\mathsf{ctr} \in \mathbb{Z}_T$. Let

$$(\mathsf{ct} = c_1 \dots c_n, \mathsf{ctr}) \leftarrow \Pi_{\mathsf{aGM}}.\mathsf{Enc}(\mathsf{ap}, \mathsf{M}, \widehat{\mathsf{M}}, \mathsf{dk}, \mathsf{ctr})$$

for a covert plaintext $\widehat{\mathsf{M}} = \widehat{m}_1 \dots \widehat{m}_n \in \{0,1\}^n$ and normal plaintext $\mathsf{M} = m_1 \dots m_n \in \{0,1\}^n$ where $\forall i \in [n]$, $c_i = y_i^2 x^{m_i} \bmod N$ with $y_i = F(K, (\mathsf{ctr}, i, m_i \oplus \widehat{m}_i))$.

The correctness of the normal decryption follows from the correctness of Π_{GM}. Since $c_i = y_i^2 x^{m_i}$ with $y_i \in \mathbb{Z}_N^*$; hence lines 1–8 of Algorithm 4 give $\mathsf{M} = m_1 \dots m_n$. Then $z_i = c_i x^{-m_i} = y_i^2$ with $y_i = F(K, (\mathsf{ctr}, i, \beta_i))$ for $\beta_i = m_i \oplus \widehat{m}_i$.
Position i is decoded correctly when the test $z_i = F(K, (\mathsf{ctr}, i, 0))^2$ is true exactly if $\beta_i = 0$. If $\beta_i = 0$ the test succeeds and $\widehat{\gamma}_i = m_i = \widehat{m}_i$.
If $\beta_i = 1$ the first test fails unless $F(K, (\mathsf{ctr}, i, 0))^2 = F(K, (\mathsf{ctr}, i, 1))^2$ and then the second test succeeds and $\widehat{\gamma}_i = 1 - m_i = \widehat{m}_i$.
So decoding fails only if for some i the two squares coincide. For independent uniform $u, u' \in \mathbb{Z}_N^*$ we have

$$\Pr[u^2 = u'^2] = 4/\Phi(N) \leq 2^{-(2\lambda-4)}$$

(u' must be one of four square roots of u^2). Considering the $2n$ points $\{(\mathsf{ctr}, i, \beta) \mid i \in [n], \beta \in \{0,1\}\}$, if some pair $(\mathsf{ctr}, i, 0), (\mathsf{ctr}, i, 1)$ collides, the decoding will fail. Therefore, the correctness can fail with probability at most $n2^{-(2\lambda-4)}$. Hence, $\Pr[\widehat{\Gamma} \neq \widehat{\mathsf{M}}] \leq n\, 2^{-(2\lambda-4)}$. □

Theorem 3 *The AE Π_{aGM} of Goldwasser-Micali cryptosystem Π_{GM} is computationally robust: for every $\mathsf{M} \in \{0,1\}^n$ a normal ciphertext decrypts anamorphically to a covert plaintext with probability at most $2^{-(2\lambda-5)n}$.*

Proof Let

$$\begin{aligned}
&\mathsf{pp} = \mathcal{G}_\lambda \leftarrow \Pi_{\mathsf{GM}}.\mathsf{Setup}(1^\lambda)\\
&(\mathsf{sk} = (p,q), \mathsf{pk} = (N,x)) \leftarrow \Pi_{\mathsf{GM}}.\mathsf{Gen}(\mathsf{pp})\\
&\mathsf{ap} = F \leftarrow \Pi_{\mathsf{aGM}}.\mathsf{Setup}(\mathsf{pk})\\
&(\mathsf{dk} = (K, \mathsf{pk}), \mathsf{ctr}) \leftarrow \Pi_{\mathsf{aGM}}.\mathsf{Gen}(\mathsf{ap}, \mathsf{pk})
\end{aligned}$$

where λ is security parameter, $\mathcal{G}_\lambda$ is a λ-bit prime generator, p, q are two λ-bit primes generated by $\mathcal{G}_\lambda$, $N = pq$, $x \in \mathsf{PQR}(N)$ is a PQR modulo N, $F : \{0,1\}^\nu \times (\mathbb{Z}_T \times [n] \times \{0,1\}) \to \mathbb{Z}_N^*$ is a PRF, $K \in \{0,1\}^\nu$, $\mathsf{ctr} \in \mathbb{Z}_T$. Let

$$\mathsf{ct} = c_1 \dots c_n \leftarrow \Pi_{\mathsf{GM}}.\mathsf{Enc}(\mathsf{pp}, \mathsf{M}, \mathsf{pk})$$

be the normal ciphertext of the message $\mathsf{M} = m_1 \dots m_n \in \{0,1\}^n$ where $c_i = y_i^2 x^{m_i} \bmod N$ for uniformly random $y_i \in \mathbb{Z}_N^*$ for all $i \in [n]$.
The decoder of Algorithm 4 recovers m_i correctly and obtains $z_i = y_i^2$. Squaring is a 4-to-1 homomorphism of $\mathbb{Z}_N^*$ onto $\Delta_2 = \mathsf{QR}(N)$. So, z_i is uniform on $\mathsf{QR}(N)$ and independent of dk and of the other z_j. Now, $|\mathsf{QR}(N)| = \Phi(N)/4$. The decoder accepts position i only if $z_i \in \{F(K,(\mathsf{ctr},i,0))^2, F(K,(\mathsf{ctr},i,1))^2\}$, two fixed elements. Therefore, it happens with probability at most

$$\frac{2}{|\mathsf{QR}(N)|} = \frac{8}{\Phi(N)} = \frac{8}{(p-1)(q-1)}$$

The decoder returns a covert plaintext only if all n positions are accepted, so by independence

$$\Pr\left[\widehat{\Gamma} \neq \perp\right] \leq \left(\frac{8}{(p-1)(q-1)}\right)^n$$

As p, q are λ-bit primes,

$$\begin{aligned}
& p-1, q-1 \geq 2^{\lambda-1}\\
\implies\ & (p-1)(q-1) \geq 2^{2\lambda-2}\\
\implies\ & \frac{8}{(p-1)(q-1)} \leq \frac{8}{2^{2\lambda-2}} = 2^{5-2\lambda}\\
\implies\ & \left(\frac{8}{(p-1)(q-1)}\right)^n \leq 2^{-(2\lambda-5)n}
\end{aligned}$$

Hence, $\Pr\left[\widehat{\Gamma} \neq \perp\right] \leq 2^{-(2\lambda-5)n}$, negligible in λ. □

Theorem 4 *The AE Π_{aGM} is IND-NA secure as per Def. 8. For every distinguisher $\mathcal{D}$ that makes at most q encryption queries there is a PRF adversary $\mathcal{D}'$ making at most nq queries such that*

$$\mathsf{Adv}^{\mathsf{IND\text{-}NA}}_{\Pi_{\mathsf{aGM}},\mathcal{D}}(\lambda) \leq \mathsf{Adv}^{\mathsf{PRF}}_{F,\mathcal{D}'}(\lambda) \leq \mathsf{Adv}^{\mathsf{PRF}}_{G,\mathcal{D}''}(\lambda) + nq(2^{-\xi} + 2^{-\lambda+2})$$

where $q < T$.

Proof We describe below the security game $\mathsf{Game}_0 = \mathsf{Exp}^{\mathsf{IND\text{-}NA}}_{\mathsf{aGM},\mathcal{D}}(\lambda)$ between a challenger $\mathbf{C}$ and a distinguisher $\mathcal{D}$ following Fig. 3.
The challenger generates the public parameter $\mathsf{pp} = \mathcal{G}_\lambda \leftarrow \Pi_{\mathsf{GM}}.\mathsf{Setup}(1^\lambda)$, a secret key and public key pair $(\mathsf{sk} = (p,q), \mathsf{pk} = (N,x)) \leftarrow \Pi_{\mathsf{GM}}.\mathsf{Gen}(\mathsf{pp})$, the anamorphic public parameter $\mathsf{ap} = F \leftarrow \Pi_{\mathsf{aGM}}.\mathsf{Setup}(\mathsf{pk})$ and the double key-counter pair $(\mathsf{dk} = (K, \mathsf{pk}), \mathsf{ctr}) \leftarrow \Pi_{\mathsf{aGM}}.\mathsf{Gen}(\mathsf{ap}, \mathsf{pk})$ and sends $(\mathsf{pp}, \mathsf{sk}, \mathsf{pk})$ to the distinguisher $\mathcal{D}$. Here $\mathcal{G}_\lambda$ is a prime number generator, p, q are λ-bit prime numbers generated by $\mathcal{G}_\lambda$, $N = pq$ and $x \in \mathsf{PQR}(N)$ is a PQR modulo N, $F : \{0,1\}^\nu \times (\mathbb{Z}_T \times [n] \times \{0,1\}) \to \mathbb{Z}_N^*$ is a PRF, $K \in \{0,1\}^\nu$, $\mathsf{ctr} \in \mathbb{Z}_T$. The challenger $\mathbf{C}$ samples $b \xleftarrow{\$} \{0,1\}$ and answers the queries $(\mathsf{M}, \widehat{\mathsf{M}})$ of $\mathcal{D}$ with the ciphertext $\mathsf{ct} = c_1 \dots c_n$ where $c_i = y_i^2 x^{m_i}$ with

$$\begin{array}{ll} y_i \xleftarrow{\$} \mathbb{Z}_N^* & \text{if } b = 0 \\ y_i = F(K, (\mathsf{ctr}, i, m_i \oplus \widehat{m}_i)) & \text{if } b = 1 \end{array}$$

where ctr is incremented after each query when $b = 1$. Finally, the adversary $\mathcal{D}$ returns a bit $b' \in \{0,1\}$ and wins iff $b' = b$.
Let Game_1 be same as Game_0 except $F(K,\cdot)$ replaced by a uniformly random function $f : \mathbb{Z}_T \times [n] \times \{0,1\} \to \mathbb{Z}_N^*$. Let E_i be the event that $\mathcal{D}$ wins Game_i for $i \in \{0,1\}$, i.e. outputs $b' = b$.

Claim 1. $|\Pr[E_0] - \Pr[E_1]| \le \mathsf{Adv}^{\mathsf{PRF}}_{F,\mathcal{D}'}(\lambda)$.

Proof The PRF adversary $\mathcal{D}'$ is given an oracle $\mathcal{O}(\cdot)$ of either the PRF $F(K,\cdot)$ or a uniformly random function $f(\cdot)$.
It generates

$$\begin{array}{l} \mathsf{pp} = \mathcal{G}_\lambda \leftarrow \Pi_{\mathsf{GM}}.\mathsf{Setup}(1^\lambda) \\ (\mathsf{sk} = (p,q), \mathsf{pk} = (N,x)) \leftarrow \Pi_{\mathsf{GM}}.\mathsf{Gen}(\mathsf{pp}) \end{array}$$

itself, samples a counter $\mathsf{ctr} \xleftarrow{\$} \mathbb{Z}_T$ sends $(\mathsf{pp}, \mathsf{sk}, \mathsf{pk})$ to $\mathcal{D}$, samples $b \xleftarrow{\$} \{0,1\}$ and answers each query $(\mathsf{M}, \widehat{\mathsf{M}})$ as above with a ciphertext $\mathsf{ct} = c_1 \dots c_n$ with $c_i = y_i^2 x^{m_i} \bmod N$ where

$$\begin{array}{ll} y_i \xleftarrow{\$} \mathbb{Z}_N^* & \text{if } b = 0 \\ y_i = \mathcal{O}(\mathsf{ctr}, i, (m_i \oplus \widehat{m}_i)) & \text{if } b = 1 \end{array}$$

(incrementing ctr by 1 mod T for $b = 1$).
When $\mathcal{D}$ outputs b', $\mathcal{D}'$ outputs 1 iff $b' = b$. If $\mathcal{O}(\cdot)$ is for the PRF $F(K,\cdot)$, the simulation is Game_0 and $\mathcal{D}'$ outputs 1 with probability $\Pr[E_0]$. If $\mathcal{O}(\cdot)$ is for the random function $f(\cdot)$, it is Game_1 and the probability is $\Pr[E_1]$. The difference of the two acceptance probabilities is bounded by $\mathsf{Adv}^{\mathsf{PRF}}_{F,\mathcal{D}'}(\lambda)$ (Def. 11). Therefore, $|\Pr[E_0] - \Pr[E_1]| \le \mathsf{Adv}^{\mathsf{PRF}}_{F,\mathcal{D}'}(\lambda)$. □

Claim 2. $\Pr[E_1] = \frac{1}{2}$.

Proof The counter takes q distinct values $\mathsf{ctr}, \mathsf{ctr}+1, \dots$ modulo T since $q < T$ and the positions inside one query are distinct, so every point (ctr, i, β) at which f is evaluated is fresh (each point is used at most once, whatever the value of β). A uniform random function takes independent uniform values at distinct points, so in Game_1 with $b = 1$ all y_i over the whole game are independent and uniform on $\mathbb{Z}_N^*$, whatever the bits $m_i \oplus \widehat{m}_i$ chosen by $\mathcal{D}$. This is exactly the distribution of the y_i for $b = 0$.
Therefore, the view of $\mathcal{D}$ has the same distribution for $b = 0$ and $b = 1$ and $\mathcal{D}$ guesses b correctly with probability exactly $\frac{1}{2}$. □

Consequently,

$$\mathsf{Adv}^{\mathsf{IND\text{-}NA}}_{\Pi_{\mathsf{aGM}},\mathcal{D}}(\lambda) = |\Pr[E_0] - \frac{1}{2}| = |\Pr[E_0] - \Pr[E_1]| \leq \mathsf{Adv}^{\mathsf{PRF}}_{F,\mathcal{D}'}(\lambda)$$

and Lemma 1 gives the second inequality. □

4 Our construction Π_{aBen}: synchronous AE from Benaloh PKE

Let Π_{Ben} be the Benaloh PKE associated with the plaintext space $\mathcal{M} = \mathbb{Z}_r$ and the ciphertext space $\mathcal{C} = \mathbb{Z}_N^*$ where r is a prime and $N = pq$ for λ-bit primes p, q satisfying $r \mid (p-1), r^2 \nmid (p-1), r \nmid (q-1)$. Each user generates $\mathsf{pk} = (y, N)$ and $\mathsf{sk} = (\phi, x)$ with $\phi = (p-1)(q-1)$, $y \in \mathbb{Z}_N^*$ and $x = y^{\phi/r} \bmod N \neq 1$; since ϕ can be recomputed from (p, q) we also write $\mathsf{sk} = (p, q, x)$. The ciphertext of $\mathsf{M} \in \mathbb{Z}_r$ is $\mathsf{ct} = y^{\mathsf{M}} u^r \bmod N$ with $u \xleftarrow{\$} \mathbb{Z}_N^*$ and decryption computes $\mathsf{M}' = \log_x(\mathsf{ct}^{\phi/r} \bmod N) \in \mathbb{Z}_r$.

Notation. $\Delta_r = \{a^r \mid a \in \mathbb{Z}_N^*\}$, so $|\Delta_r| = \Phi(N)/r$. The randomness component u^r of a Benaloh ciphertext is a uniform element of Δ_r. We use the PRF $F^{(r)} = (\sigma_r \circ (\psi_N \circ G)) : \{0,1\}^\nu \times \mathbb{Z}_T \to \Delta_r$ with $F^{(r)}(K, \mathsf{ctr}) = (\psi_N \circ G(K, \mathsf{ctr}))^r \in \Delta_r$ (Lemma 1); $F^{(r)}$ is computed by one r-th power, which anybody can do without the factorization of N. The covert plaintext space is $\widehat{\mathcal{M}} = \{0,1\}^\ell$ with $\ell = \lambda - 2 - \tau$ and the embedding of a string s into Δ_r is

$$e(s) = \mathsf{int}(s) \cdot 2^\tau + 1 \in [1, 2^{\lambda-2}), \qquad \eta(s) = e(s)^r \bmod N \in \Delta_r$$

Since $e(s) < 2^{\lambda-2} < \min(p, q)$, $e(s)$ is coprime to N and $e(s) \in \mathbb{Z}_N^*$. The set of valid encodings is $V = \{t2^\tau + 1 : 0 \leq t < 2^\ell\}$. The next lemma shows that $\eta(s)$ is uniquely decodable by the receiver and that all the ambiguity of r-th roots sits in the prime p.

Lemma 5. (i) $\mu_r = \{a \in \mathbb{Z}_N^* : a^r = 1\} = \langle x \rangle$ has order r. (ii) If $a \in \mu_r$, $a = 1 \bmod q$. (iii) Let $t = r^{-1} \bmod (q-1)$. For all $a \in \mathbb{Z}_N^*$, $(a^r \bmod q)^t = a \bmod q$. (iv) If Γ is uniform on Δ_r then $\Gamma \bmod q$ is uniform on $\mathbb{Z}_q^*$.

Proof (i) $x^r = y^\phi = 1$ and $x \neq 1$ with r prime, so x has order r and $x \in \mu_r$. By the Chinese remainder theorem

$$|\mu_r| = |\{a \in \mathbb{Z}_p^* : a^r = 1\}| \cdot |\{a \in \mathbb{Z}_q^* : a^r = 1\}| = r \cdot 1$$

because $r \mid p-1$ and $\gcd(r, q-1) = 1$; so $\mu_r = \langle x \rangle$.
(ii) For $a \in \mu_r$, $a \bmod q$ satisfies $a^r = 1$ in $\mathbb{Z}_q^*$ where $a \mapsto a^r$ is bijective as $\gcd(r, q-1) = 1$. Hence, $a^r = 1 \bmod q \implies a = 1 \bmod q$.
(iii) Such a t exists as $\gcd(r, q-1) = 1$ and $rt = 1 \bmod q-1 \implies rt = 1 + k(q-1)$ for some integer k. Therefore, by Fermat's theorem,

$$(a^r \bmod q)^t = a^{rt} \bmod q = a^{1+k(q-1)} = a \bmod q$$

(iv) By the Chinese remainder theorem $\Delta_r = \Delta \times \mathbb{Z}_q^*$ where Δ is the group of r-th powers in $\mathbb{Z}_p^*$, because r-th powering is bijective on $\mathbb{Z}_q^*$. □

Hence $\Lambda(\Gamma)$: *compute* $w = (\Gamma \bmod q)^t \bmod q$*; if* $w \in V$ *output* $\mathsf{int}^{-1}((w-1)/2^\tau)$, *else* $\perp$ satisfies

$$\Lambda(\eta(s)) = s$$

The four algorithms of Π_{aBen} are as follows.

- The algorithm $\Pi_{\mathsf{aBen}}.\mathsf{Setup}$ described in Algorithm 5 may be run by any party (sender, receiver or an authority). It sets the anamorphic parameter ap which is just the description of the PRF $F = \psi_N \circ G : \{0,1\}^\nu \times \mathbb{Z}_T \to \mathbb{Z}_N^*$; no secret randomness is involved and $G : \{0,1\}^\nu \times \mathbb{Z}_T \to \{0,1\}^{2\lambda+\xi}$ can be a fixed public standard.

Algorithm 5 $\Pi_{\mathsf{aBen}}.\mathsf{Setup}(\mathsf{pk}) \to \mathsf{ap}$

1: $\mathsf{ap} = F = \psi_N \circ G$ with G a fixed public PRF;

- The algorithm $\Pi_{\mathsf{aBen}}.\mathsf{Gen}$, presented in Algorithm 6 run by the sender (resp. the receiver), samples a ν-bit PRF key K and an initial counter $\mathsf{ctr} \xleftarrow{\$} \mathbb{Z}_T$ and sets $\mathsf{dk} = (K, \mathsf{pk})$. Then $(\mathsf{dk}, \mathsf{ctr})$ is passed to the receiver (resp. the sender) over a secure channel.

Algorithm 6 $\Pi_{\mathsf{aBen}}.\mathsf{Gen}(\mathsf{ap}, \mathsf{pk}) \to (\mathsf{dk}, \mathsf{ctr})$

1: $K \xleftarrow{\$} \{0,1\}^\nu$; $\mathsf{ctr} \xleftarrow{\$} \mathbb{Z}_T$;
2: $\mathsf{dk} = (K, \mathsf{pk} = (y, N))$;

- The algorithm $\Pi_{\mathsf{aBen}}.\mathsf{Enc}$ described in Algorithm 7 is run by the sender on input the ap, normal message $\mathsf{M} \in \mathbb{Z}_r$, a covert message $\widehat{\mathsf{M}} \in \{0,1\}^\ell$, the double key dk and the current counter ctr. It returns a ciphertext ct and an updated counter $\mathsf{ctr} = \mathsf{ctr} + 1 \bmod T$.

Algorithm 7 $\Pi_{\mathsf{aBen}}.\mathsf{Enc}(\mathsf{ap}, \mathsf{M}, \widehat{\mathsf{M}}, \mathsf{dk}, \mathsf{ctr}) \to (\mathsf{ct}, \mathsf{ctr})$

1: $\psi = F(K, \mathsf{ctr})$; $u = e(\widehat{\mathsf{M}}) \cdot \psi \bmod N$;
2: $\mathsf{ct} = y^{\mathsf{M}}\, u^r \bmod N$; $\triangleright = y^{\mathsf{M}}\, \eta(\widehat{\mathsf{M}})\, F^{(r)}(K, \mathsf{ctr})$
3: $\mathsf{ctr} = \mathsf{ctr} + 1 \bmod T$;

- The algorithm $\Pi_{\mathsf{aBen}}.\mathsf{Dec}$ given in Algorithm 8 is run by the receiver on input anamorhic parameter ap, a ciphertext $\mathsf{ct} \in \mathbb{Z}_N^*$, secret key $\mathsf{sk} = (\phi, x)$, double key $\mathsf{dk} = (K, \mathsf{pk})$ and the current counter ctr. It recovers $\widehat{\Gamma}$ and an updated counter ctr.

The receiver divides by ψ modulo q only, which is cheaper than inverting $F^{(r)}$ modulo N and gives the same result (Lemma 5(iii)).

Theorem 6 Π_{aBen} *is correct:* $\Pr[\widehat{\Gamma} = \widehat{\mathsf{M}}] = 1$ *and normal decryption of an anamorphic ciphertext returns* M.

Algorithm 8 $\Pi_{\mathsf{aBen}}.\mathsf{Dec}(\mathsf{ap}, \mathsf{ct}, \mathsf{sk}, \mathsf{dk}, \mathsf{ctr}) \to (\widehat{\Gamma}, \mathsf{ctr})$

1: $a = \mathsf{ct}^{\phi/r} \bmod N$; find $\mathsf{M} \in \mathbb{Z}_r$ with $x^{\mathsf{M}} = a$ (scan $\leq r$ multiplications, baby-step giant-step, or a table); if none, $\widehat{\Gamma} = \perp$;
2: $\Gamma' = \mathsf{ct}\,(y^{-1})^{\mathsf{M}} \bmod N$; $w = (\Gamma' \bmod q)^t \bmod q$;
3: $\psi = F(K, \mathsf{ctr})$; $e' = w\,(\psi \bmod q)^{-1} \bmod q$;
4: **if** $e' \in V$ **then**
5: $\quad \widehat{\Gamma} = \mathsf{int}^{-1}((e'-1)/2^{\tau})$;
6: **else**
7: $\quad \widehat{\Gamma} = \perp$;
8: **end if**
9: $\mathsf{ctr} = \mathsf{ctr} + 1 \bmod T$;

Proof Let

$$\begin{aligned}&\mathsf{pp} = \mathcal{G}_\lambda \leftarrow \Pi_{\mathsf{Ben}}.\mathsf{Setup}(1^\lambda)\\ &(\mathsf{sk} = (\phi, x), \mathsf{pk} = (y, N)) \leftarrow \Pi_{\mathsf{Ben}}.\mathsf{Gen}(\mathsf{pp})\\ &\mathsf{ap} = F \leftarrow \Pi_{\mathsf{aBen}}.\mathsf{Setup}(\mathsf{pk})\\ &(\mathsf{dk} = (K, \mathsf{pk} = (y, N)), \mathsf{ctr}) \leftarrow \Pi_{\mathsf{aBen}}.\mathsf{Gen}(\mathsf{ap}, \mathsf{pk})\end{aligned}$$

where λ is the security parameter, $\mathcal{G}_\lambda$ is large λ-bit prime-pair generator that generates prime numbers p, q such that $r \mid (p-1), r^2 \nmid (p-1), r \nmid (q-1)$, r (prime) is the plaintext space size, $\phi = \Phi(N) = (p-1)(q-1)$, $y \in \mathbb{Z}_N^*$ such that $y^{\phi/r} \neq 1 \bmod N$ and $x = y^{\phi/r} \bmod N$, $F = \psi_N \circ G : \{0,1\}^\nu \times \mathbb{Z}_T \to \mathbb{Z}_N^*$ is a PRF, $K \in \{0,1\}^\nu$ and $\mathsf{ctr} \in \mathbb{Z}_T$ is the initial counter. By Algorithm 7, $\mathsf{ct} = y^{\mathsf{M}}(e\psi)^r \bmod N$ with $e = e(\widehat{\mathsf{M}})$, $\psi = F(K, \mathsf{ctr})$ and $e\psi \in \mathbb{Z}_N^*$. Then

$$\mathsf{ct}^{\phi/r} \bmod N = x^{\mathsf{M}}(e\psi)^\phi \bmod N = x^{\mathsf{M}} \bmod N$$

So, the recovered normal plaintext is M (line 1; same as $\Pi_{\mathsf{Ben}}.\mathsf{Dec}$). Therefore, $\Gamma' = (e\psi)^r \bmod N$ and by Lemma 5(iii),

$$w = (\Gamma' \bmod q)^t \bmod q = e\psi \bmod q$$

So, $e' = w\psi^{-1} \bmod q = e \bmod q$.
As $1 \leq e < 2^{\lambda-2} < q$, $e' = e \in V$ and $\widehat{\Gamma} = \widehat{\mathsf{M}}$. □

Theorem 7 Π_{aBen} *is computationally robust: for every* $\mathsf{M} \in \mathbb{Z}_r$*, a normal ciphertext decrypts anamorphically to a covert plaintext with probability at most* $2^\ell/(q-1) \leq 2^{-\tau-1}$.

Proof Let

$$\begin{aligned}&\mathsf{pp} = \mathcal{G}_\lambda \leftarrow \Pi_{\mathsf{Ben}}.\mathsf{Setup}(1^\lambda)\\ &(\mathsf{sk} = (\phi, x), \mathsf{pk} = (y, N)) \leftarrow \Pi_{\mathsf{Ben}}.\mathsf{Gen}(\mathsf{pp})\\ &\mathsf{ap} = F \leftarrow \Pi_{\mathsf{aBen}}.\mathsf{Setup}(\mathsf{pk})\\ &(\mathsf{dk} = (K, \mathsf{pk} = (y, N)), \mathsf{ctr}) \leftarrow \Pi_{\mathsf{aBen}}.\mathsf{Gen}(\mathsf{ap}, \mathsf{pk})\end{aligned}$$

where λ is the security parameter, $\mathcal{G}_\lambda$ is large λ-bit prime-pair generator that generates prime numbers p, q such that $r \mid (p-1), r^2 \nmid (p-1), r \nmid (q-1)$, r (prime) is the plaintext space size, $\phi = \Phi(N) = (p-1)(q-1)$, $y \in \mathbb{Z}_N^*$ such that $y^{\phi/r} \neq 1 \bmod N$ and $x = y^{\phi/r} \bmod N$, $F = \psi_N \circ G : \{0,1\}^\nu \times \mathbb{Z}_T \to \mathbb{Z}_N^*$ is a PRF, $K \in \{0,1\}^\nu$ and $\mathsf{ctr} \in \mathbb{Z}_T$ is the initial counter. Let

$$\mathsf{ct} = y^{\mathsf{M}} u^r \leftarrow \Pi_{\mathsf{Ben}}.\mathsf{Enc}(\mathsf{pp}, \mathsf{M}, \mathsf{pk})$$

be the normal ciphertext of the message $\mathsf{M} \in \mathbb{Z}_r$ with $u \xleftarrow{\$} \mathbb{Z}_N^*$. The decoder of Algorithm 8 recovers M in Line 1 and $\Gamma' = u^r$ is uniform on Δ_r, independent of K and ctr.
By Lemma 5(iv),(iii) $w = (\Gamma' \bmod q)^t \bmod q$ is uniform on $\mathbb{Z}_q^*$ and so is $e' = w\psi^{-1} \bmod q$ for fixed $\psi = F(K, \mathsf{ctr})$.
The decoder accepts iff $e' \in V$ and $|V| = 2^\ell$. Therefore, the decoder returns a covert message with probability at most $\dfrac{|V|}{(q-1)} = \dfrac{2^\ell}{(q-1)} \le \dfrac{2^{\lambda-2-\tau}}{2^{\lambda-1}} = 2^{-\tau-1}$. □

Theorem 8 Π_{aBen} *is IND-NA secure as per Def. 8. For every distinguisher* $\mathcal{D}$ *making at most* $q < T$ *encryption queries there are PRF adversaries* $\mathcal{D}', \mathcal{D}''$ *such that*

$$\mathsf{Adv}^{\mathsf{IND\text{-}NA}}_{\Pi_{\mathsf{aBen}},\mathcal{D}}(\lambda) \le \mathsf{Adv}^{\mathsf{PRF}}_{F^{(r)},\mathcal{D}'}(\lambda) \le \mathsf{Adv}^{\mathsf{PRF}}_{G,\mathcal{D}''}(\lambda) + q(2^{-\xi} + 2^{-\lambda+2})$$

Proof We describe below the security game $\mathsf{Game}_0 = \mathsf{Exp}^{\mathsf{IND\text{-}NA}}_{\mathsf{aBen},\mathcal{D}}(\lambda)$ between a challenger $\mathbf{C}$ and a distinguisher $\mathcal{D}$ following Fig. 3.
The challenger generates the public parameter $\mathsf{pp} = \mathcal{G}_\lambda \leftarrow \Pi_{\mathsf{Ben}}.\mathsf{Setup}(1^\lambda)$, a secret key and public key pair $(\mathsf{sk} = (\phi, x), \mathsf{pk} = (y, N)) \leftarrow \Pi_{\mathsf{Ben}}.\mathsf{Gen}(\mathsf{pp})$, the anamorphic public parameter $\mathsf{ap} = F \leftarrow \Pi_{\mathsf{aBen}}.\mathsf{Setup}(\mathsf{pk})$ and the double key-counter pair $(\mathsf{dk} = (K, \mathsf{pk}), \mathsf{ctr}) \leftarrow \Pi_{\mathsf{aBen}}.\mathsf{Gen}(\mathsf{ap}, \mathsf{pk})$ and sends $(\mathsf{pp}, \mathsf{sk}, \mathsf{pk})$ to the distinguisher $\mathcal{D}$. Here $\mathcal{G}_\lambda$ generates λ-bit prime-pairs p, q such that $r \mid (p-1), r^2 \nmid (p-1), r \nmid (q-1)$ for a prime number r being the plaintext space size, (p, q) is a prime-pair generated by $\mathcal{G}_\lambda$, $N = pq$, $\phi = \Phi(N) = (p-1)(q-1)$, $y \in \mathbb{Z}_N^*$ such that $y^{\phi/r} \not\equiv 1 \bmod N$, $x = y^{\phi/r} \bmod N$, $F = \psi_N \circ G : \{0,1\}^\nu \times \mathbb{Z}_T \to \mathbb{Z}_N^*$ is a PRF, $F^{(r)} : \{0,1\}^\nu \times \mathbb{Z}_T \to \Delta_r$ is the r-th power PRF of F, $K \in \{0,1\}^\nu$, $\mathsf{ctr} \in \mathbb{Z}_T$.

The challenger $\mathbf{C}$ samples a bit $b \xleftarrow{\$} \{0,1\}$ and answers the queries $(\mathsf{M}, \widehat{\mathsf{M}})$ of the adversary $\mathcal{D}$ with the ciphertext $\mathsf{ct} = y^{\mathsf{M}}\widehat{u} \in \mathbb{Z}_N^*$ with

$$\begin{array}{ll} \widehat{u} = u^r, \quad u \xleftarrow{\$} \mathbb{Z}_N^* & \text{if } b = 0 \\ \widehat{u} = \eta(\widehat{\mathsf{M}}) \cdot F^{(r)}(K, \mathsf{ctr}) & \text{if } b = 1 \end{array}$$

ctr being incremented after each such query if $b = 1$.
We define Game_1 to be same as Game_0 except that $F^{(r)} : \{0,1\}^\nu \times \mathbb{Z}_T \to \Delta_r$ is replaced by a uniformly random function $f : \mathbb{Z}_T \to \Delta_r$.
As in the proof of Theorem 4, a PRF adversary $\mathcal{D}'$ that simulates the game Game_0 or Game_1 with its oracle and outputs 1 iff $\mathcal{D}$ wins, yields

$$|\Pr[E_0] - \Pr[E_1]| \le \mathsf{Adv}^{\mathsf{PRF}}_{F^{(r)},\mathcal{D}'}(\lambda)$$

In Game_1 the q values of ctr are distinct, so the values $f(\mathsf{ctr})$ are independent and uniform on Δ_r; multiplication by the fixed element $\eta(\widehat{\mathsf{M}}) \in \Delta_r$ permutes Δ_r, so $\widehat{u}$ is uniform on Δ_r, independently of $\widehat{\mathsf{M}}$, which is the distribution for $b = 0$. Thus, $\Pr[E_1] = \frac{1}{2}$. Consequently,

$$\mathsf{Adv}^{\mathsf{IND\text{-}NA}}_{\Pi_{\mathsf{aBen}},\mathcal{D}}(\lambda) = \left|\Pr[E_0] - \frac{1}{2}\right| = |\Pr[E_0] - \Pr[E_1]| \le \mathsf{Adv}^{\mathsf{PRF}}_{F^{(r)},\mathcal{D}'}(\lambda)$$

and the second inequality follows with Lemma 1. □

Remark 3. The normal plaintext of Π_{Ben} has only $\log_2 r$ bits, because decryption costs $O(r)$ multiplications. So, the bandwidth rate $\alpha = \ell/\log_2 r \gg 1$ and the covert rate $\varrho = \ell/\log_2 N \approx 0.46$ show its better performance.

5 Deniability, synchronization and further security analysis

5.1 Key deniability

In the dictatorial setting, the dictator holds $(\mathsf{pp}, \mathsf{pk}, \mathsf{sk})$ and may obtain a double key from a coerced sender. The receiver's defense is that anybody can produce a valid double key for pk, so a double key found in the dictator's hands is no evidence about the receiver.

Definition 12 (Key deniability) An AE Π_{aPKE} is *key-deniable* if there is a PPT algorithm Sim taking only $(\mathsf{pp}, \mathsf{pk})$ such that for every distinguisher $\mathcal{D}$ (even computationally unbounded)

$$|\Pr[\mathcal{D}(\mathsf{pp}, \mathsf{pk}, \mathsf{sk}, \mathsf{ap}, \mathsf{dk}, \mathsf{ctr}) = 1] - \Pr[\mathcal{D}(\mathsf{pp}, \mathsf{pk}, \mathsf{sk}, \mathsf{Sim}(\mathsf{pp}, \mathsf{pk})) = 1]| \leq \mathsf{neg}(\lambda)$$

where $\mathsf{pp} \leftarrow \mathsf{Setup}(1^\lambda)$, $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen}(\mathsf{pp})$ and $(\mathsf{ap}, \mathsf{dk}, \mathsf{ctr})$ is the triple the receiver holds, which is produced by $\Pi_{\mathsf{aPKE}}.\mathsf{Setup}$ and $\Pi_{\mathsf{aPKE}}.\mathsf{Gen}$ run by either party. The distribution of $(\mathsf{ap}, \mathsf{dk}, \mathsf{ctr})$ is thus independent of sk given pk.

Theorem 9 *Π_{aGM}, Π_{aBen} and the schemes of Section 6 are key-deniable with $\mathsf{Sim} = (\mathsf{Setup}, \mathsf{Gen})$, with advantage 0.*

Proof In Π_{aGM} and Π_{aBen}, the algorithm Setup takes only pk and outputs a public PRF description. Also, the algorithm Gen takes $(\mathsf{ap}, \mathsf{pk})$ as input and samples a PRF key $K \xleftarrow{\$} \{0,1\}^\nu$ and an initial counter $\mathsf{ctr} \xleftarrow{\$} \mathbb{Z}_T$ independently of sk (Algorithms 2, 6).
Hence, the triple produced by the receiver, by the sender or by Sim has the same distribution given $(\mathsf{pp}, \mathsf{pk}, \mathsf{sk})$ and the advantage is 0 for any distinguisher $\mathcal{D}$. □

This property distinguishes the extensions from asymmetric anamorphic schemes in which the double key is generated together with the receiver's key pair and depends on sk.

Remark 4 (What is *not* claimed). Deniability is plausible deniability of *ownership*. (i) A dictator holding dk can recognise and decode the anamorphic ciphertexts that were sent under it; this is inherent in any symmetric double key and the sender is exposed. (ii) A receiver whose device is searched and contains dk and ctr is exposed. (iii) We do not define deniability of the covert plaintext against a dictator who holds dk (equivocation) and do not obtain it.
The *forward-secure variant* below limits the damage of (i) to ciphertexts sent *after* the key was captured.

5.2 Lossy networks: windowed decryption

The dictator controls the network and can drop, delay or reorder ciphertexts, so the counters of sender and receiver can drift apart. The schemes are *synchronized* (stateful) and need the following mechanism. The windowed decryption Dec_W

takes the receiver's counter c and a window $W \geq 1$ and runs Dec with counters $c, c+1, \ldots, c+W-1$ in turn (for Π_{aGM} the normal decryption and the Legendre symbols are computed once). It returns the first result different from $\perp$, together with the counter $c+j+1$, or $\perp$ and the unchanged counter. Messages delayed beyond the window, or reordered behind later ones, are lost unless the receiver keeps a bitmap of skipped counters in the style of *Internet Protocol Security* (IPsec) anti-replay.

Proposition 10 (Resilience to loss) *Suppose the receiver holds counter c and the next ciphertext to arrive was produced with counter $c+\delta$, $0 \leq \delta < W$. Then Dec_W returns the covert plaintext and the counter $c+\delta+1$ except with probability at most $\varepsilon_{\mathsf{cor}} + \delta\,(\theta + \mathsf{Adv}_F^{\mathsf{PRF}}(\lambda))$, where $\varepsilon_{\mathsf{cor}}$ is the correctness failure probability and θ is the robustness failure probability of the AE.*
Specifically, $\varepsilon \leq n\,2^{-(2\lambda-4)}$, $\theta \leq 2^{-(2\lambda-5)n}$ for Π_{aGM} and $\varepsilon = 0$, $\theta = 2^{-\tau-1}$ for Π_{aBen}.

Proof Counter $c+\delta$ decodes correctly except with probability $\varepsilon_{\mathsf{cor}}$.
Each earlier counter $c+j$, $j < \delta$, must not accept falsely that happens except with probability θ. Replace F by a random function which costs $\mathsf{Adv}_F^{\mathsf{PRF}}(\lambda)$ per counter. Then the PRF values at counter $c+j$ are independent of those used by the encryption. The union bound $j < \delta$ yields that Dec_W returns the covert message and the counter $c+\delta+1$ except with probability at most $\varepsilon_{\mathsf{cor}} + \delta(\theta + \mathsf{Adv}_F^{\mathsf{PRF}}(\lambda))$.
The correctness failure probability is $\varepsilon_{\mathsf{cor}} \leq n\,2^{-(2\lambda-4)}$ for Π_{aGM} (Theorem 2) and $\varepsilon_{\mathsf{cor}} = 0$ for Π_{aBen} (Theorem 6).
For Π_{aGM}, $z_i = y_i^2$, $y_i = F(K, (c+\delta, i, m_i \oplus \widehat{m}_i))$ (for the counter $c+\delta$) is uniform on $\mathsf{QR}(N)$ and independent of the two squares $\{F(K,(c+j,i,0))^2, F(K,(c+j,i,1))^2\}$ tested. So, the argument of Theorem 3 gives the probability of false acceptance to be $\theta = \left(\frac{2}{|\mathsf{QR}(N)|}\right)^n \leq 2^{-(2\lambda-5)n}$.
For Π_{aBen}, $e' = e\,\psi_{c+\delta}\,\psi_{c+j}^{-1} \bmod q$ is uniform on $\mathbb{Z}_q^*$ and the argument of Theorem 7 gives the false acceptance probability $\theta = \frac{|V|}{q-1} \leq 2^{-\tau-1}$. □

Hence a window W needs $\tau \geq \log_2 W + \kappa$ for κ bits of false-acceptance security in the Benaloh schemes; with $\tau = 128$ and $W = 2^{20}$ the loss is negligible. The Dec_W cost is W PRF evaluations in the worst case. If more than $W-1$ consecutive ciphertexts are lost the parties must resynchronize over the secure channel by a new $(\mathsf{dk}, \mathsf{ctr})$.

5.3 Counter reuse and state rollback

Proposition 11 (Counter reuse breaks IND-NA) *Consider the IND-NA experiment in which, in addition, the distinguisher may ask the oracle to restore the counter to an earlier value (modeling a virtual-machine snapshot or a crash after sending). Then there is a distinguisher $\mathcal{D}$ against Π_{aGM} with advantage at least $\frac{1}{2} - \frac{1}{2}(2^{-(2\lambda-4)})^n$ and one against Π_{aBen} with advantage at least $\frac{1}{2} - \frac{1}{2|\Delta_r|}$.*

Proof $\mathcal{D}$ asks the query $(\mathsf{M}, \widehat{\mathsf{M}})$, restores the counter and asks the same query again. For $b = 1$ both ciphertexts are equal, since the encryption is deterministic given (K, ctr). For $b = 0$, the encryption randomness will be changed and the ciphertexts will be equal only with some negligible probability. The adversary $\mathcal{D}$ outputs 1 iff the ciphertexts are equal and wins with probability $1 - \frac{1}{2}\Pr[\text{equal} \mid b = 0]$. therefore, the advantage of $\mathcal{D}$ is

$$\mathsf{Adv}^{\mathsf{IND\text{-}NA}}_{\Pi_{\mathsf{aPKE}},\mathcal{D}}(\lambda) = \left|(1 - \frac{1}{2}\Pr[\text{equal} \mid b = 0]) - \frac{1}{2}\right| = \frac{1}{2} - \frac{1}{2}\Pr[\text{equal} \mid b = 0]$$

For Π_{aGM} scheme, when $b = 0$, each component of two independent normal ciphertexts coincides with probability $4/\Phi(N) \leq 2^{-(2\lambda-4)}$. Therefore, two independent normal ciphertexts (n components) coincides with probability $\Pr[\text{equal} \mid b = 0] \leq (2^{-(2\lambda-4)})^n$.

For Π_{aBen} scheme, when $b = 0$, $\Pr[\text{equal} \mid b = 0] \leq \dfrac{1}{|\Delta_r|}$.

Hence, $\mathsf{Adv}^{\mathsf{IND\text{-}NA}}_{\Pi_{\mathsf{aGM}},\mathcal{D}}(\lambda) \geq \dfrac{1}{2} - \dfrac{1}{2}(2^{-(2\lambda-4)})^n$ and $\mathsf{Adv}^{\mathsf{IND\text{-}NA}}_{\Pi_{\mathsf{aBen}},\mathcal{D}}(\lambda) \geq \dfrac{1}{2} - \dfrac{1}{2|\Delta_r|}$. □

Counter reuse is the practical weak point of every synchronized AE, including [3]. The sender must write the incremented counter to persistent storage *before* the ciphertext is released (write-ahead) and must not restore the counter from a backup. We do not know a way to remove the assumption without giving up the stateless-impossibility barrier [8] or without sending a nonce, which would be visible to the dictator.

5.4 IND-CPA of the anamorphic mode, many keys and the scope of IND-NA

Corollary 12 (IND-CPA of the anamorphic mode) Let $\mathsf{Exp}^{\mathsf{CPA\text{-}a}}$ be the IND-CPA experiment of Def. 4 in which the challenge ciphertext is the anamorphic encryption $\Pi_{\mathsf{aPKE}}.\mathsf{Enc}(\mathsf{ap}, m^*_b, \widehat{\mathsf{M}}, \mathsf{dk}, \mathsf{ctr})$ for a covert plaintext $\widehat{\mathsf{M}}$ chosen by the adversary $\mathcal{A}$ (who does not know dk). Then

$$\mathsf{Adv}^{\mathsf{IND\text{-}CPA\text{-}a}}_{\Pi_{\mathsf{aPKE}},\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\Pi_{\mathsf{PKE}},\mathcal{B}}(\lambda) + 2\,\mathsf{Adv}^{\mathsf{IND\text{-}NA}}_{\Pi_{\mathsf{aPKE}},\mathcal{D}}(\lambda)$$

for suitable IND-CPA adversary $\mathcal{B}$ and IND-NA adversary $\mathcal{D}$.

Proof The IND-NA challenger $\mathbf{C}$ produces the public parameter $\mathsf{pp} \leftarrow \Pi_{\mathsf{PKE}}.\mathsf{Setup}(1^\lambda)$, the key pair $(\mathsf{sk}, \mathsf{pk}) \leftarrow \Pi_{\mathsf{PKE}}.\mathsf{Gen}(\mathsf{pp})$, the anamorphic parameter $\mathsf{ap} \leftarrow \Pi_{\mathsf{aPKE}}.\mathsf{Setup}(\mathsf{pk})$, the double key and counter pair $(\mathsf{dk}, \mathsf{ctr}) \leftarrow \Pi_{\mathsf{aPKE}}.\mathsf{Gen}(\mathsf{ap}, \mathsf{pk})$ and samples a bit $b \xleftarrow{\$} \{0, 1\}$.
The adversary $\mathcal{D}$ gets the triplet $(\mathsf{pp}, \mathsf{sk}, \mathsf{pk})$ from the challenger $\mathbf{C}$, passes pp, pk to the adversary $\mathcal{A}$ and runs $\mathcal{A}$. On the encryption challenge $(m^*_0, m^*_1, \widehat{\mathsf{M}})$ from $\mathcal{A}$, the adversary $\mathcal{D}$ queries its oracle (given by $\mathbf{C}$) once on $(m^*_{b^*}, \widehat{\mathsf{M}})$ with its own random bit b^*, gets the challenge ciphertext ct and passes ct to $\mathcal{A}$ where

$$\begin{array}{ll} \mathsf{ct} \leftarrow \Pi_{\mathsf{PKE}}.\mathsf{Enc}(\mathsf{pp}, m^*_{b^*}, \mathsf{pk}) & \text{if } b = 0 \\ (\mathsf{ct}, \mathsf{ctr}) \leftarrow \Pi_{\mathsf{aPKE}}.\mathsf{Enc}(\mathsf{ap}, m^*_{b^*}, \widehat{\mathsf{M}}, \mathsf{dk}, \mathsf{ctr}) & \text{if } b = 1 \end{array}$$

Then, $\mathcal{D}$ outputs $b' = 1$ iff $\mathcal{A}$ guesses b^*.
If p_a and p_n are the success probabilities of $\mathcal{A}$ with anamorphic ($b = 1$ case) and normal challenge ($b = 0$ case), $\mathcal{D}$ wins with probability $\frac{1}{2}(1 - p_n) + \frac{1}{2}p_a$. So,

$$\mathsf{Adv}^{\mathsf{IND\text{-}NA}}_{\Pi_{\mathsf{aPKE}},\mathcal{D}}(\lambda) = \left|(\frac{1}{2}(1 - p_n) + \frac{1}{2}p_a) - \frac{1}{2}\right| = \frac{1}{2}\,|p_a - p_n|$$

With a normal challenge, $\mathcal{A}$ is an IND-CPA adversary $\mathcal{B}$ against Π_{PKE}, which is secure under QRP (Goldwasser-Micali), rRP (Benaloh) and DCRA (Paillier). Therefore,

$$\begin{aligned} 2\mathsf{Adv}^{\mathsf{IND\text{-}NA}}_{\Pi_{\mathsf{aPKE}},\mathcal{D}}(\lambda) &= |p_a - p_n| = \left|(p_a - \frac{1}{2}) - (p_n - \frac{1}{2})\right| \\ &\geq \left|(p_a - \frac{1}{2})\right| - \left|(p_n - \frac{1}{2})\right| = \mathsf{Adv}^{\mathsf{IND\text{-}CPA\text{-}a}}_{\Pi_{\mathsf{aPKE}},\mathcal{A}}(\lambda) - \mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\Pi_{\mathsf{PKE}},\mathcal{B}}(\lambda) \end{aligned}$$

Hence, $\mathsf{Adv}^{\mathsf{IND\text{-}CPA\text{-}a}}_{\Pi_{\mathsf{aPKE}},\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{\mathsf{IND\text{-}CPA}}_{\Pi_{\mathsf{PKE}},\mathcal{B}}(\lambda) + 2\,\mathsf{Adv}^{\mathsf{IND\text{-}NA}}_{\Pi_{\mathsf{aPKE}},\mathcal{D}}(\lambda)$. □

Proposition 13 (Many double keys) *Let $\mathcal{D}$ interact with μ instances, each with an independent double key and counter for the same or independent key pairs, ask queries to any of them and receive all secret keys. Then $\mathsf{Adv}^{\mathsf{IND\text{-}NA\text{-}}\mu}_{\Pi_{\mathsf{aPKE}},\mathcal{D}}(\lambda) \leq \mu \cdot \max_{\mathcal{D}'} \mathsf{Adv}^{\mathsf{IND\text{-}NA}}_{\Pi_{\mathsf{aPKE}},\mathcal{D}'}(\lambda)$, with a bound for the concrete schemes of $\mu(\mathsf{Adv}^{\mathsf{PRF}}_{F,\mathcal{D}''}(\lambda) + nq(2^{-\xi} + 2^{-\lambda+2}))$ as in Theorems 4 and 8.*

Proof Use hybrids H_t, $0 \leq t \leq \mu$, in which the first t instances answer the encryption queries from the normal oracle and the others from the anamorphic oracle. H_0 and H_μ are the two worlds and neighbouring hybrids (H_i, H_{i+1} for $0 \leq i \leq t-1$) differ in one instance only; the other instances can be simulated by the reduction since they depend on independent keys that it chooses itself. □

Remark 5 (Active adversaries). IND-NA is a CPA-style notion: the adversary sees ciphertexts but does not modify or inject them. Goldwasser-Micali, Benaloh and Paillier are malleable. A dictator can multiply a ciphertext by an element of Δ_r and thereby change or destroy the covert plaintext (for instance, multiplying by v^r with $v = 1 \bmod 2^\tau$ for small v can still yield a valid encoding) and he can replay old ciphertexts.
Replays and injections of random ciphertexts are rejected with probability $1 - 2^{-\tau-1}$ by the redundancy tag and by the counter; targeted malleation is not prevented. A MAC under a key derived from K and placed inside the covert plaintext prevents it at the price of $|\mathsf{tag}|$ payload bits. We do not model an anamorphic CCA notion in this paper; the normal mode has the usual homomorphic malleability of the base PKE.

5.5 Forward-secure variant: coerced senders

The dictator may coerce the sender after the fact and obtain the sender's *current state*. With a fixed K this exposes all earlier covert traffic whose ciphertexts the dictator stored. We replace (K, ctr) by a one-way chain. Let $P : \{0,1\}^\nu \to \{0,1\}^{2\nu}$ be a *pseudorandom generator* (PRG), for instance $P(s) = (\mathsf{HMAC}_s(0), \mathsf{HMAC}_s(1))$ truncated (HMAC denotes a hash-based message authentication code). The state is $\mathsf{st}_0 = K$; for message j the sender computes $(\mathsf{st}_{j+1}, k_j) = P(\mathsf{st}_j)$, encrypts with the PRF key k_j (and the counter $\mathsf{ctr} + j$ as index) and erases st_j, k_j. The receiver does the same. For Dec_W it ratchets forward and keeps the skipped keys only if it wants to accept reordered messages.

Theorem 14 (Forward-secure IND-NA) *Let* Π^{fs} *be* Π_{aGM} *or* Π_{aBen} *with the chain above. Consider the IND-NA experiment in which, after* q *queries,* $\mathcal{D}$ *also receives the current state* st_q *(in both worlds the chain is advanced once per query). Then* $\mathsf{Adv}^{\mathsf{IND\text{-}NA}}_{\Pi^{\mathsf{fs}},\mathcal{D}}(\lambda) \le q\,(\mathsf{Adv}^{\mathsf{PRG}}_{P}(\lambda) + \mathsf{Adv}^{\mathsf{PRF}}_{F}(\lambda))$ *for suitable adversaries.*

Proof Hybrid H_j: the pairs (st_{i+1}, k_i) for $i < j$ are independent uniform, the rest are computed from the uniform st_j. $H_j \to H_{j+1}$ replaces $P(\mathsf{st}_j)$ by a uniform pair, which costs $\mathsf{Adv}^{\mathsf{PRG}}_{P}(\lambda)$ (st_j is uniform in H_j).
In H_q the state st_q given to $\mathcal{D}$ and the keys $k_0, \ldots, k_{q-1}$ are independent uniform strings. Replace the PRFs $F(k_i, \cdot)$ one by one by independent random functions; each key is used for one query only, so each step costs $\mathsf{Adv}^{\mathsf{PRF}}_{F}(\lambda)$. All randomness $y_i \in \mathbb{Z}_N^*$ (in Π_{aGM}), respectively $u \in \mathbb{Z}_N^*$ (in Π_{aBen}), is then fresh and uniform as in the proofs of Theorems 4 and 8, independent of b and of st_q.
Hence, $\mathsf{Adv}^{\mathsf{IND\text{-}NA}}_{\Pi^{\mathsf{fs}},\mathcal{D}}(\lambda) \le q\,(\mathsf{Adv}^{\mathsf{PRG}}_{P}(\lambda) + \mathsf{Adv}^{\mathsf{PRF}}_{F}(\lambda))$. □

Since the ciphertexts of the anamorphic world are indistinguishable from normal ones even given st_q and sk, the covert plaintexts sent before the capture stay hidden. This protects against a dictator who coerces the sender; it does not protect messages sent after the capture.

6 A framework of Δ-structured PKEs and new schemes

The two constructions above use one fact: the randomness of the ciphertext is a uniform element of a subgroup Δ that the sender can sample and multiply and the receiver can decode a payload from Δ. We now state this as a framework.

Definition 13 (Δ-structured PKE) A PKE Π is Δ-structured if, for every pk, the following are efficiently computable from pk unless stated otherwise.

(1) A finite abelian group $\mathfrak{G} \supseteq \mathcal{C}$ (containing the ciphertext space $\mathcal{C}$) and a subgroup $\Delta \le \mathfrak{G}$ and a map $\epsilon : \mathcal{M} \to \mathfrak{G}$ such that $\mathsf{Enc}(\mathsf{pp}, \mathsf{M}, \mathsf{pk}) = \epsilon(\mathsf{M}) \cdot \delta$ with δ uniform on Δ and Dec recovers M from every element of the coset $\epsilon(\mathsf{M})\Delta$ (so the cosets are pairwise disjoint).

(2) A sampler of Δ from random bits within statistical distance ε_Δ of uniform: $\delta = \sigma_{\mathsf{pk}}(F)$ obtained from a PRF output as in Lemma 1, i.e. $\Delta = \{u^e : u \in \mathbb{Z}_N^*\}$ is the image of a homomorphism computable from pk.

(3) A finite set $\mathcal{S}$ (the covert plaintext space) with an injective map $\eta : \mathcal{S} \to \Delta$ and a map $\Lambda_{\mathsf{sk}} : \Delta \to \mathcal{S} \cup \{\perp\}$ computable from sk with $\Lambda_{\mathsf{sk}}(\eta(s)) = s$. Let $\theta = \Pr_{\delta \leftarrow \Delta}[\Lambda_{\mathsf{sk}}(\delta) \neq \perp]$ be the false acceptance density.

The generic AE $\Pi_{\mathsf{a}}[\Pi]$ with $\mathsf{dk} = (K, \mathsf{pk})$ and counter $\mathsf{ctr} \in \mathbb{Z}_T$ is: The anamorphic encryption algorithm $\Pi_{\mathsf{a}}.\mathsf{Enc}$ outputs $\mathsf{ct} = \epsilon(\mathsf{M}) \cdot \eta(\widehat{\mathsf{M}}) \cdot F^{\Delta}(K, \mathsf{ctr})$ and increments ctr. The anamorphic decryption algorithm $\Pi_{\mathsf{a}}.\mathsf{Dec}$ recovers M following $\Pi.\mathsf{Dec}$, computes $\Gamma = \mathsf{ct} \cdot \epsilon(\mathsf{M})^{-1} \cdot F^{\Delta}(K, \mathsf{ctr})^{-1}$ and outputs $\Lambda_{\mathsf{sk}}(\Gamma)$. For messages made of n independent components (bit-wise PKEs) component i uses $F^{\Delta}(K, (\mathsf{ctr}, i))$ instead of $F^{\Delta}(K, \mathsf{ctr})$.

Theorem 15 *Let Π be Δ-structured. Then $\Pi_{\mathsf{a}}[\Pi]$ (1) is correct with probability 1 and normal decryption of an anamorphic ciphertext returns M; (2) is computationally robust: a normal ciphertext anamorphically decodes with probability θ (per component); (3) is IND-NA secure with*

$$\mathsf{Adv}^{\mathsf{IND\text{-}NA}}_{\Pi_{\mathsf{a}},\mathcal{D}}(\lambda) \le \mathsf{Adv}^{\mathsf{PRF}}_{F^{\Delta}}(\lambda) \le \mathsf{Adv}^{\mathsf{PRF}}_{G}(\lambda) + nq\,\varepsilon_{\Delta}$$

for $q < T$ queries of n components; (4) is key-deniable (Theorem 9); (5) satisfies Proposition 10 with false-acceptance probability θ per wrong counter and Theorem 14.

Proof (1) The anamorphic ciphertext is $\mathsf{ct} = \epsilon(\mathsf{M}) \cdot \eta(\widehat{\mathsf{M}}) \cdot F^{\Delta}(K, \mathsf{ctr}) \in \epsilon(\mathsf{M})\Delta$ since $\eta(\widehat{\mathsf{M}})F^{\Delta} \in \Delta$. So, M is recovered (Def. 13). Now,

$$\Gamma = \mathsf{ct} \cdot \epsilon(\mathsf{M})^{-1} \cdot F^{\Delta}(K, \mathsf{ctr})^{-1} = \eta(\widehat{\mathsf{M}})$$

Therefore, $\Lambda_{\mathsf{sk}}(\Gamma) = \widehat{\mathsf{M}}$.
(2) For a normal ciphertext $\mathsf{ct} = \epsilon(\mathsf{M})\delta$,

$$\Gamma = \mathsf{ct} \cdot \epsilon(\mathsf{M})^{-1} \cdot F^{\Delta}(K, \mathsf{ctr})^{-1} = \delta F^{\Delta}(K, \mathsf{ctr})^{-1}$$

is uniform on Δ because δ is uniform and independent of K. Hence, $\Pr[\Lambda_{\mathsf{sk}}(\Gamma) \neq \perp] = \theta$.
(3) As in Theorems 4 and 8: replace $F^{\Delta}(K, \cdot)$ by a random function into Δ; all inputs are distinct, so the values are independent and identically distributed and uniform on Δ. Then multiplication by the fixed $\eta(\widehat{\mathsf{M}}) \in \Delta$ preserves uniformity, so the anamorphic ciphertext is distributed as $\epsilon(\mathsf{M})\delta$ with δ uniform, as the normal one.
(4),(5) are as before. □

Instances. Π_{aGM} is the instance of bit-wise construction with $\mathfrak{G} = \mathbb{Z}_N^*$, $\Delta = \{y^2 | y \in \mathbb{Z}_N^*\}$, $\epsilon(m) = x^m \bmod N$, $\theta \le 2^{-(2\lambda-5)n}$ for an n-bit message.
Π_{aBen} is the instance with $\mathfrak{G} = \mathbb{Z}_N^*$, $\Delta = \{u^r | u \in \mathbb{Z}_N^*\}$, $\epsilon(\mathsf{M}) = y^{\mathsf{M}} \bmod N$, $\theta \le 2^{-\tau-1}$.
The following are new.

6.1 Block Goldwasser-Micali AE Π_{aGMb}

Take $p, q = 3 \bmod 4$ (or use Tonelli-Shanks). $\mathfrak{G} = \mathbb{Z}_N^*$, $\Delta = \Delta_2 = \mathsf{QR}(N)$, $\epsilon(m) = x^m$, $m \in \{0,1\}$ (the cosets $\mathsf{QR}(N)$ and $x\mathsf{QR}(N)$ are separated by the Legendre symbol modulo p), $F : \{0,1\}^{\nu} \times (\mathbb{Z}_T \times [n]) \to \mathbb{Z}_N^*$ is a PRF same as Π_{aGM}, $F^{\Delta} = F^{(2)}$ is defined by $F^{(2)}(K, (\mathsf{ctr}, i)) = F(K, (\mathsf{ctr}, i))^2$, $\mathcal{S} = \{0,1\}^{\ell}$ with

$$e(s) = \mathsf{int}(s) \cdot 2^{\tau} + 1 \in [1, 2^{\lambda-2}), \quad \eta(s) = e(s)^2 \bmod N \in \Delta_2$$

$\forall s \in \{0,1\}^{\ell}$ where $\ell = \lambda - 2 - \tau$ similar to that of Π_{aBen}.
$\Lambda(\Gamma)$: The decoder Λ computes the two square roots $\pm w \in \mathbb{Z}_q$ of Γ mod q and outputs the valid one (that lies in $V = \{t2^{\tau} + 1 | 0 \le t < 2^{\ell}\}$). Both cannot be valid, because if $w \in V \implies w < 2^{\lambda-2}$, then $q - w > 2^{\lambda-2} \implies q - w \notin V$. Therefore,

$$\Lambda(\eta(s)) = s \quad \forall s \in \{0,1\}^{\ell}$$

Thus, *each bit-ciphertext $c_i = x^{m_i}(e(s_i)\psi_i)^2$ for $\psi_i = F(K, (\mathsf{ctr}, i))$ carries a covert payload of $\ell = \lambda - 2 - \tau$ bits instead of one.*
For a uniform $\Gamma \in \mathsf{QR}(N)$ the residue modulo q is uniform on $\mathsf{QR}(q)$ where $|\mathsf{QR}(q)| =$

$(q-1)/2$ and the accepted set is $V = \{t2^\tau + 1 | 0 \le t < 2^\ell\}$ with $|V| = 2^\ell$ distinct squares, so the false acceptance probability is

$$\theta = \frac{|V|}{(q-1)/2} = \frac{2|V|}{(q-1)} \le \frac{2 \cdot 2^\ell}{2^{\lambda-1}} = \frac{2^{1+\lambda-2-\tau}}{2^{\lambda-1}} = 2^{-\tau}$$

per element. Hence, for every $\mathsf{M} \in \{0,1\}^n$ a normal ciphertext decrypts anamorphically to a covert plaintext with probability at most $2^{-n\tau}$.
The covert rate is $\varrho = \ell / \log_2 N \approx 0.46$ against $1/\log_2 N$ for Π_{aGM} and the result is robust and IND-NA by Theorem 15. The bit-flip scheme Π_{aGM} remains useful when only a PRF and Legendre symbols are wanted and $\widehat{\mathcal{M}} = \mathcal{M}$ is required.

6.2 Paillier and Damgård-Jurik AE Π_{aPai}

The Damgård-Jurik cryptosystem associates with the plaintext space $\mathcal{M} = \mathbb{Z}_{N^s}$, ciphertext space $\mathcal{C} = \mathbb{Z}^*_{N^{s+1}}$ for $s \ge 1$ where $N = pq$ with λ-bit primes p, q ($\gcd(N, \Phi(N)) = 1$). Let $\mathfrak{G} = \mathbb{Z}^*_{N^{s+1}}$. The public key of the user is $\mathsf{pk} = (N, s)$ and the corresponding secret key is $\mathsf{sk} = (p, q, d)$ where $d = 1 \bmod N^s$ and $d = 0 \bmod L$ for $L = \mathsf{lcm}(p-1, q-1)$. A sender encrypts a message M by computing

$$\mathsf{ct} = (1+N)^{\mathsf{M}} u^{N^s} \bmod N^{s+1}$$

for a random $u \xleftarrow{\$} \mathbb{Z}^*_N$. Here, $\epsilon(\mathsf{M}) = (1+N)^{\mathsf{M}}$ and $\Delta = \Delta_{N^s} = \{u^{N^s} | u \in \mathbb{Z}^*_N\}$ and $\mathsf{ct} \in \epsilon(\mathsf{M})\Delta$. For $s = 1$, it is the Paillier scheme. The receiver decrypts the ciphertext ct by first computing

$$\mathsf{ct}^d \bmod N^{s+1} = (1+N)^{\mathsf{M}} \bmod N^{s+1}$$

and then recovering the exponent M efficiently using recursive method.
The map $\sigma_{N^s} : \mathbb{Z}^*_N \to \mathbb{Z}^*_{N^{s+1}}$ with $\sigma_{N^s}(u) = u^{N^s} \bmod N^{s+1}$ from $\mathbb{Z}^*_N$ is an injective homomorphism (it depends on $u \bmod N$ only and $u^{N^s} = 1 \bmod N$ forces $u = 1 \bmod N$ since $\gcd(N^s, \Phi(N)) = 1$), so $|\Delta| = \Phi(N)$, sampling is exact and $\Delta \cap \langle 1+N \rangle = \{1\}$ separates the cosets. Normal message recovery is done by the Damgård-Jurik decryption. For the payload, let

$$e(s) = \mathsf{int}(s)2^\tau + 1 < 2^{2\lambda-3}, \quad \eta(s) = e(s)^{N^s}$$

$\forall s \in \{0,1\}^{\ell_P}$ with $\ell_P = 2\lambda - 3 - \tau$.
$\Lambda(\Gamma)$: The decoder Λ computes

$$w = (\Gamma \bmod N)^{(N^s)^{-1} \bmod \Phi(N)} \bmod N$$

and outputs the payload if $w \in V$, else $\perp$.
The root $w \in \mathbb{Z}^*_N$ is *unique*, so the whole $\mathbb{Z}^*_N$ is usable, not just the residue modulo one prime. For a uniform Γ the root is uniform on $\mathbb{Z}^*_N$ and $\theta = 2^{\ell_P}/\Phi(N) \le 2^{-\tau}$.
A payload $e(s)$ can fail to be a unit only if $e(s) \in \{p, q\} \cdot \mathbb{Z}$, i.e. if it reveals a factor

of N. The covert plaintext space is $\{s : \gcd(e(s), N) = 1\}$, which contains all but at most $2^{-\lambda+3}$ of all strings. The scheme costs one Paillier encryption/decryption plus one PRF and one root extraction ($\varrho \approx 0.48$ for $s = 1$, $\approx \frac{1}{s+1} \cdot 0.96$ in general). Because M may have $\log_2 N$ bits the bandwidth rate $\alpha \approx 1$ while ϱ is the largest in our family.

Remark 6 (Other residuosity PKEs). Okamoto-Uchiyama needs a decodable embedding of strings into $\langle g^N \rangle$, whose group order is unknown to the sender and whose discrete logarithm is not available to the receiver in general; Naccache-Stern has a composite plaintext modulus dividing both $p-1$ and $q-1$, so that the unique-decoding argument of Lemma 5(ii) fails. We do not claim extensions for these two and regard them as open.

7 Conclusion

We studied anamorphic extensions (AEs) of residuosity-based PKEs whose ciphertexts carry a recoverable, group-structured randomness component. The central idea is to replace this randomness by a PRF output that encodes the covert message, so that the receiver recovers the covert message from the ciphertext itself. This gives AEs of the Goldwasser-Micali and Benaloh PKEs whose double key is a single 128-bit PRF key. The bit-wise Goldwasser-Micali AE has bandwidth rate 1 and is computationally robust with false-acceptance probability at most $2^{-(2\lambda-5)n}$. The Benaloh AE uses an explicit embedding of bit strings into the group of r-th powers with unique decoding; a τ-bit redundancy tag makes it robust. All IND-NA proofs reduce to the security of the PRF, with an explicit loss for sampling into the group.

The framework of Δ-structured PKEs turns these two instances into a method. It yields new high-rate AEs from block Goldwasser-Micali, Paillier and Damgård-Jurik, with covert rate $\varrho \approx 0.46$–0.48 at the 128-bit security level, against 0.0026 (finite-field) and 0.031 (elliptic-curve) for an ElGamal-based AE with 16 covert bits. The paper also addresses the operational side of synchronised extensions: a formal notion of key deniability, windowed decryption on a lossy network, a proof that counter reuse breaks IND-NA, IND-CPA security of the anamorphic mode, security with many double keys, and a forward-secure variant that protects earlier covert traffic when a sender is coerced.

Declarations

Conflict of interest: The authors declare that they have no conflicts of interest to report regarding the present paper.

References

[1] Persiano, G., Phan, D.H., Yung, M.: Anamorphic encryption: private communication against a dictator. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 34–63. Springer, Cham (2022)

[2] Naor, M., Yung, M.: Public-key cryptosystems provably secure against chosen ciphertext attacks. In: Proceedings of the Twenty-second Annual ACM Symposium on Theory of Computing, pp. 427–437. Association for Computing Machinery, New York, USA (1990)

[3] Banfi, F., Gegier, K., Hirt, M., Maurer, U., Rito, G.: Anamorphic encryption, revisited. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 3–32. Springer, Cham (2024)

[4] ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information theory **31**(4), 469–472 (1985)

[5] Cramer, R., Shoup, V.: A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Annual International Cryptology Conference, pp. 13–25. Springer, Berlin, Heidelberg (1998)

[6] Bellare, M., Rogaway, P.: Optimal asymmetric encryption. In: Workshop on the Theory and Application of of Cryptographic Techniques, pp. 92–111. Springer, Berlin, Heidelberg (1994)

[7] Catalano, D., Giunta, E., Migliaro, F.: Anamorphic encryption: New constructions and homomorphic realizations. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 33–62. Springer, Cham (2024)

[8] Catalano, D., Giunta, E., Migliaro, F.: Generic anamorphic encryption, revisited: New limitations and constructions. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 275–303. Springer, Cham (2025)

[9] Persiano, G., Phan, D.H., Yung, M.: Public-key anamorphism in (cca-secure) public-key encryption and beyond. In: Annual International Cryptology Conference, pp. 422–455. Springer, Cham (2024)

[10] Dodis, Y., Goldin, E.: Anamorphic-resistant encryption; or why the encryption debate is still alive. In: Annual International Cryptology Conference, pp. 440–471. Springer, Cham (2025)

[11] Carnemolla, D., Catalano, D., Giunta, E., Migliaro, F.: Anamorphic resistant encryption: the good, the bad and the ugly. In: Annual International Cryptology Conference, pp. 472–503. Springer, Cham (2025)

[12] Kutylowski, M., Persiano, G., Phan, D.H., Yung, M., Zawada, M.: The self-anti-censorship nature of encryption: On the prevalence of anamorphic cryptography. Proceedings on Privacy Enhancing Technologies **2023**(4), 170–183 (2023)

[13] Chakraborty, N., Dutta, R.: Bandwidth-efficient anamorphic extension with provable security from blum-goldwasser cryptosystem. In: Proceedings of the ACM ASIA Public-Key Cryptography Workshop, pp. 21–30 (2026)

[14] Banerjee, S., Pal, T., Rupp, A., Slamanig, D.: Simple public key anamorphic encryption and signature using multi-message extensions. IACR Cryptol. ePrint Arch. **2025**, 370 (2025)

[15] Pleşca, C., Togan, M., Lupaşcu, C.: Homomorphic encryption based on group algebras and goldwasser-micali scheme. In: International Conference for Information Technology and Communications, pp. 149–166. Springer, Cham (2016)

[16] Koç, Ç.K., Özdemir, F., Ödemiş Özger, Z.: Benaloh algorithm. In: Partially Homomorphic Encryption, pp. 63–69. Springer, Cham (2021)

[17] Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In: International Conference on the Theory and Applications of Cryptographic Techniques, pp. 223–238 (1999). Springer

[18] Damgård, I., Jurik, M.: A generalisation, a simplification and some applications of paillier's probabilistic public-key system. In: International Workshop on Public Key Cryptography, pp. 119–136 (2001). Springer

[19] Okamoto, T., Uchiyama, S.: A new public-key cryptosystem as secure as factoring. In: International Conference on the Theory and Applications of Cryptographic Techniques, pp. 308–318 (1998). Springer

[20] Naccache, D., Stern, J.: A new public key cryptosystem based on higher residues. In: Proceedings of the 5th ACM Conference on Computer and Communications Security, pp. 59–66 (1998)