Computational Quantum Anamorphic Encryption and Anamorphic Secret Sharing

Sayantan Ganguly[1,2], Shion Samadder Chaudhury[1]

Abstract

The concept of anamorphic encryption, first formally introduced by Persiano et al. in their influential 2022 paper titled "Anamorphic Encryption: Private Communication Against a Dictator," enables embedding covert messages within ciphertexts. One of the key distinctions between a ciphertext embedding a covert message and an original ciphertext, compared to an anamorphic ciphertext, lies in the indistinguishability between the original ciphertext and the anamorphic ciphertext. This encryption procedure has been defined based on a public-key cryptosystem. Initially, we present a quantum analogue of the classical anamorphic encryption definition that is based on public-key encryption. Additionally, we introduce a definition of quantum anamorphic encryption that relies on symmetric key encryption. Furthermore, we provide a detailed generalized construction of quantum anamorphic symmetric key encryption within a general framework, which involves taking any two quantum density matrices of any different dimensions and constructing a single quantum density matrix, which is the quantum anamorphic ciphertext containing ciphertexts of both of them. Subsequently, we introduce a definition of computational anamorphic secret-sharing and extend the work of Çakan et al. on computational quantum secret-sharing to computational quantum anamorphic secret-sharing, specifically addressing scenarios with multiple messages, multiple keys, and a single share function. This proposed secret-sharing scheme demonstrates impeccable security measures against quantum adversaries.

Index Terms

Anamorphic Encryption, Quantum Anamorphic Public-Key Encryption, Quantum Symmetric Key Encryption, Anamorphic Secret Sharing, Computational Quantum Anamorphic Secret-Sharing.

CONTENTS

Contents

[1] Department of Cryptology, Institute for Advancing Intelligence (IAI), TCG CREST, EP & GP Block, Sector - V, Salt Lake, Kolkata-700091, West Bengal, India.
[2] Department of Computer Science, Ramakrishna Mission Vivekananda Educational and Research Institute (RKMVERI), Belur, West Bengal, India.
Corresponding Author Email: sayantan.ganguly.90@tcgcrest.org
Corresponding Author Email: chaudhury.shion@gmail.com

I. Introduction

With the advent of quantum computing, the field of cryptography is experiencing an unprecedented paradigm shift [1], [2]. Quantum communication systems have several crucial advantages compared to classical cryptographic and communicational methods [3]. These advantages stem from the unique properties of quantum mechanics, enabling new forms of security and computational capabilities that classical systems cannot provide [4]. Quantum communication offers several advantages over classical communication systems, mainly in terms of its security and efficiency [5]. A key quantum communication advantage is unconditional security, which is especially suitable for QKD applications that cannot be guaranteed by any classical communication system [6]. The no-cloning theorem states that under quantum communication, it is not possible to copy an unknown quantum state exactly [7]. Quantum communication is a very important thread in the framework for quantum computing systems [8]. With quantum computation, quantum communication allows for exponential gains in processing large datasets or complex algorithms [9]. Quantum communication is expected to be the backbone of the quantum networks spreading the quantum states among distributed quantum computers and sensors to perform complex tasks like distributed quantum computing, quantum-enhanced sensing, and secure global QKD [10].

The word “anamorphic” characterizes a distorted or deformed projection or drawing; however, from a given point of view or technique, it seems or appears normal. Anamorphic encryption is a cryptographic encryption technique, a notion invented by Persiano et. al. [11]. According to Persiano et al. [11], its success depends on two often-taken-for-granted assumptions: sender freedom and receiver privacy. The first assumes senders can choose the message, and the second assumes the receiver’s secret key is uncompromised. While these assumptions are natural in most cases, they may be at risk in nations where law enforcement can force users to hand over their decryption keys. In dictatorships, citizens may only communicate regime-approved content, diminishing the sender’s freedom [12]. Persiano et al. [11] added anamorphic encryption to these challenging cases. In [11], two primitives are proposed depending on which assumption is unreliable: Sender anamorphic encryption handles circumstances where the sender’s freedom assumption fails, whereas receiver anamorphic encryption addresses compromised private keys [12]. In an anamorphic encryption scheme, Alice can send a message to Bob, an original message and a covert message under dictatorial supervision in such a way that the original ciphertexts and the anamorphic ciphertexts are indistinguishable from the dictator [11]. One thing that makes anamorphic encryption stand out is that, unlike other steganographic methods, it can hide communication in a message that looks like any other encrypted message. It keeps the very existence of the hidden anamorphic message undetectable unless performed with the usage of the correct decryption key or method. The anamorphic message uses a special anamorphic key or protocol to decrypt it, while the original message can be decrypted through another key distinct from the anamorphic key. The existing works on classical encryption are mainly based on public-key encryption [11]–[13].

Here, we shall make a distinction between steganography and anamorphic encryption [14]. Steganography is the technique of masking information within some other unsuspecting data in such a way that even the existence of the hidden data may not be detectable [15]. A steganographic technique typically hides the original message in a *non-encrypted* cover message through images, audio, or text using subtle modifications so that it would not raise suspicions in an observer that something is being hidden [16]. The challenge is to ensure that the modifications made to the cover object do not raise suspicion [17]. This requires that the alterations are small enough to be undetectable [18]. If the cover object is examined closely, statistical analysis (e.g., using *steganalysis* techniques) might reveal the existence of hidden data [19].

The main goal of anamorphic encryption is to construct such an encryption scheme in such a way that the original ciphertext and the anamorphic ciphertext are indistinguishable from the observation of the adversary. The crucial point here is that the ciphertext looks like normal encryption, and an observer is unaware that a second covert message exists. The encryption process ensures that the ciphertext can be decrypted in two ways, depending on the key used. The challenge is to ensure that the ciphertext is *indistinguishable* from a normal ciphertext, even to an adversary who suspects that hidden messages might exist. The observer cannot tell that the ciphertext contains more than one message without the anamorphic key.

In quantum secret-sharing(QSS), a dealer distributes a secret, which is a quantum state, among the set of players. In the paper [20], Çakan et al. initiated the *computationally secure* QSS and showed that similar to the classical secret-sharing scheme, computational assumptions can significantly help in building QSS schemes. In that paper, they have constructed *polynomial-time* computationally secure QSS schemes under standard hardness assumptions for a wide class of access structures, which also includes many access structures that necessarily require exponential share size. They have also studied the class of access structures that can be implemented *efficiently* when the QSS scheme has access to a given number of copies of the secret, including all functions in P and NP [20]. Here *efficient* means both the share and the reconstruction function can be computed in polynomial time [20].

The no-cloning theorem prohibits the exact duplication of unknown quantum states [21], [22]. This implies that fundamental approaches, such as distributing identical components to multiple players, cannot be applied in quantum contexts, as the precise replication of shared states is infeasible [23], [24]. Furthermore, no quantum secret-sharing techniques currently exist to implement the OR function, which underscores the difficulty of directly adapting classical methodologies for quantum applications [25]. Consequently, essential classical outcomes, including the use of logical functions like OR, face intrinsic incompatibilities with quantum mechanics due to these constraints [26].

In this paper, we have addressed the following specific questions:

- **Question 1.** Is it possible to define an analogous quantum anamorphic encryption scheme where both the original and covert messages are represented as general quantum states or quantum density matrices of any finite dimension, while accounting for the presence of quantum adversaries?
- **Question 2.** If such a quantum anamorphic encryption scheme is feasible, how can it be constructed to securely encode general quantum density matrices?
- **Question 3.** While the classical anamorphic encryption framework is built upon public-key encryption (PKE), is it possible to develop a quantum anamorphic symmetric key encryption scheme that is secure against quantum adversaries? What are the inherent challenges in such a construction?
- **Question 4.** How can an anamorphic secret-sharing scheme be formally defined? What are the associated challenges, and what are the potential attacks that need to be considered?
- **Question 5.** How can anamorphic encryption, and consequently anamorphic secret-sharing, be designed to ensure that even if an adversary suspects the presence of a covert message, they remain incapable of decrypting it from the ciphertext?

• **Quantum advantage:** Quantum anamorphic encryption can exploit quantum superposition and entanglement to hide the existence of the inner message more effectively. For instance, quantum states can encode multiple messages simultaneously, and any attempt by an adversary to measure or intercept the message would disturb the quantum state, revealing the presence of an eavesdropper. Also, because of the no-cloning theorem, it is impossible to create an exact copy of an unknown quantum state. This property ensures that an adversary cannot clone the quantum-encrypted message to analyze it without detection. In high-stakes environments (e.g., political dissidents, and military operations), quantum anamorphic encryption provides a higher level of assurance that the hidden message cannot be detected or decrypted by a coercer, even if they have access to quantum computing resources. Quantum entanglement can be used to distribute shares of a secret in a way that any unauthorized attempt to access the shares would disrupt the entangled state, alerting the participants to the breach. Quantum systems can encode information in higher-dimensional Hilbert spaces, allowing for more efficient and secure sharing of secrets compared to classical systems. Quantum symmetric key anamorphic encryption is practical for scenarios where high-speed encryption and decryption are required, such as in real-time communication systems. The use of symmetric keys reduces computational overhead compared to public-key systems, while the quantum components ensure security against quantum attacks.

Applications: There are many real-life applications of anamorphic encryption, for example, in diplomatic or military communications, for whistleblowing, or in activism. Whether it is an autocratic regime or an environment that suppresses free speech, a journalist, activist, or whistleblower will need to air out sensitive information without the hawk-eyed views of governmental censors or repressive regimes. A whistleblower operating within one of many corrupt governmental agencies decides to leak classified documents to a journalist. In international diplomacy and military operations, sensitive communications must be kept from adversaries or other foreign intelligence agencies. Anamorphic encryption allows the diplomat or military person to send secret messages without giving away the fact that they are transmitting sensitive information. In this domain, anamorphic encryption can give added security by embedding the covert information and making it accessible only through the proper anamorphic key. Sensitive data is often stored on a third-party cloud server in cloud storage. Even if the data are encrypted, it may be in a form that the service provider can detect the existence of sensitive data, thus raising concerns about the privacy of stored information. Anamorphic encryption is one way by which data can be stored hidden without being detected by a cloud provider. A company might store business reports on a cloud server encrypted with the original key but allow the service provider to audit or perform checks. Yet those very same files can also have classified financial data or intellectual property embedded in them with the anamorphic key, whose access is limited to only the authorized personnel of the company.

A. Related Works

In classical cryptography, particularly in public-key encryption, significant progress has been made in the study of anamorphic encryption in recent years. Notable contributions include works by Banfi et al., Catalano et al., and Kutylowski [12], [13], [27]–[29], building upon its original introduction by Persiano et al. in [11]. More recently, Jaeger and Stracovsky [30] proposed additional conditions to refine the definition of anamorphic encryption. Furthermore, Wang et al. [31] presented a robust and generic construction, reformulating the concept of sender-anamorphic encryption.

In the quantum setting, there has been growing interest in quantum public-key encryption, with foundational work by Okamoto et al. [32]. More recently, Barooti et al. [33] introduced a quantum public-key encryption scheme utilizing quantum public keys, expanding the scope of secure quantum communication.

Secret-sharing plays a fundamental role in classical cryptography. For a comprehensive survey on classical secret-sharing schemes, we refer the reader to Beimel's article [34]. Efficiency is a crucial aspect of secret-sharing, ensuring that both the sharing and reconstruction processes are computationally feasible, i.e., executable in polynomial time. The seminal works of Shamir [35] and Blakley [36] introduced efficient threshold secret-sharing schemes for t-out-of-n access structures. For all functions in $\mathsf{monotone\ P}$, Yao [37] and Vinod et al. [38] developed efficient computational secret-sharing schemes. Additionally, Komargodski, Naor, and Yogev [39] constructed efficient computational secret-sharing schemes capable of realizing all functions in mNP.

In quantum cryptography, secret-sharing naturally extends to the sharing of quantum states. However, not all monotone functions permit quantum secret-sharing. The problem of quantum secret-sharing for specific classes of monotone functions has been explored in [40]–[42]. Gottesman [43] and Smith [44] provided constructions for quantum secret-sharing schemes realizing all allowable monotone functions. Imai et al. [45] proposed a general model for quantum secret-sharing, while Smith [46] constructed quantum secret-sharing schemes for general access structures. Furthermore, in [44], Smith developed quantum secret-sharing schemes for monotone functions f, ensuring that the total share size corresponds to the size of the smallest monotone span program (MSP) computing f, thus extending a classical result by Karchmer and Wigderson to the quantum domain. More recently, Çakan et al. [20] constructed and described an efficient computational model for quantum secret-sharing, further advancing this field.

B. Our Contribution

In this paper, we introduce and rigorously analyze quantum analogues of anamorphic encryption and secret-sharing in quantum communications.

Quantum Anamorphic Encryption: We propose a quantum analogous definition of the classical anamorphic encryption scheme definition in the quantum public-key encryption setting [Subsection IV, Definition 12] as well as in the quantum symmetric-key encryption setup [Subsection IV, Definition 14]. We have constructed a general quantum anamorphic symmetric-key encryption scheme [Subsection V-A] and rigorously proved the computational indistinguishability of the original ciphertext and the anamorphic ciphertext in the Theorem 11. Our construction ensures that the anamorphic ciphertext $M_f^{(1)}$, which contains both the original ciphertext and a covert ciphertext, remains indistinguishable from the original ciphertext $M_f^{(0)}$ to an adversary or to the dictator in our model. We formally established that both $M_f^{(1)}$ and $M_f^{(0)}$ are valid quantum density matrices, ensuring the integrity of our construction.

Indistinguishability and Fidelity Analysis: We demonstrate in Theorem 9 the crucial role of the multiplicative factor η in maintaining the positive semi-definiteness of the quantum density matrix $M_f^{(1)}$, showing that it is $\frac{1}{\eta}$-indistinguishable from $M_f^{(0)}$. We derived a lower bound on η in Corollary 9.1, further deriving the sufficient condition to ensure that the anamorphic ciphertext $M_f^{(1)}$ is a valid quantum density matrix. We analyzed the expected states and their computational indistinguishability (Theorem 10). Utilizing fidelity as a measure of closeness between quantum states, we establish in Theorem 12 that the fidelity between the original quantum ciphertext and the anamorphic quantum ciphertext is at least $\left(1 - \frac{1}{\eta}\right)$, indicating a high level of similarity. Also, we have analyzed the von Neumann entropy, mutual information and relative entropy for our construction and for some particular cases in [Section VIII].

Quantum Anamorphic Secret-Sharing: We propose a new definition of anamorphic secret-sharing (Definition 29) and construct a quantum anamorphic secret-sharing scheme (Theorem 14) and rigorously prove the correctness of our scheme (Theorem 15) and establish perfect privacy (Theorem 16). Our scheme generalizes the work of Çakan et al. [20] to support multiple key distributions.

Security Analysis: We analyze two potential attacks in Section VIII-B and propose countermeasures to prevent adversarial reconstruction of the covert secret. We extend Ogata et al.'s definition of cheating probability [47] to *partial cheating probability* (Definition 22) within the anamorphic secret-sharing context. We demonstrate that the adversary or dictator can be effectively prevented with high partial cheating probability (Equation 142).

C. Paper Organization

The paper is distributed among the following sections: In section II, we outline the preliminary concepts and notations required for this work. In the section III we have described the classical anamorphic encryption. We proposed a definition of quantum anamorphic public-key encryption and quantum anamorphic symmetric key encryption in IV. We present our main construction of quantum anamorphic encryption in the symmetric-key encryption setup and computational analysis in section V. The study on quantum anamorphic secret-sharing schemes is done in section VI and the compiler is presented in section VII. In section VIII, we analyze the qubit requirements, analyzed the von Neumann entropy, mutual information, relative entropy for our construction and also we have discussed some possible attacks and how to prevent it. The paper is concluded in section IX.

II. Preliminaries

A. Notations

In this paper, we have denoted non-empty sets by uppercase letters. We denote $[n] = \{1, \dots, n\}$. Let v be a vector and S be a non-empty set. We denote the symmetric group of n elements by $\mathrm{Sym}(n)$. We denote v^P to indicate the vector $(v_i)_{i \in P}$. Let $\{\mathcal{S}_i\}_{i\in[n]}$ be a family of sets, and for $P \subseteq [n]$, we denote $\mathcal{S}_P := \prod_{i \in P \subseteq [n]} \mathcal{S}_i$. For convenience, we have denoted the set of n players by $[n]$ and $\{P_1, \dots, P_n\}$ interchangeably at appropriate places. We denote $R \leftarrow \mathcal{R}$ to denote that R is uniformly distributed on $\mathcal{R}$. We used ρ to denote a density matrix acting on $\mathcal{H}$. It will be clear from the context whether we mean a vector $|\psi\rangle$ in a Hilbert space $\mathcal{H}$ representing a pure state or a density matrix ρ acting on $\mathcal{H}$, representing a mixed state. The *trace norm* $\|\cdot\|_1$ for any operator X is defined by $\|X\|_1 = \mathrm{Tr}\left(\sqrt{X^\dagger X}\right)$, with $X^\dagger$ denoting the Hermitian conjugate (or adjoint) of X. The *operator norm* of X, denoted $\|X\|$, is given by $\|X\| = \sup_{|\psi\rangle \in \mathcal{H}, \|\psi\|=1} \langle\psi|X|\psi\rangle$, where the supremum is taken over all unit vectors $|\psi\rangle \in \mathcal{H}$. If x is a vector in $\mathbb{R}^n$, its Euclidean norm is denoted $\|x\|_2$ and is defined as $\|x\|_2 = \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2}$. We denote $\log x$ as the base-2 logarithm of x, unless explicitly specified otherwise. We have used the notation P to denote different quantities in different scenarios. P may denote the set of players, the Pauli operators or the distributions. We have taken care to mention the context where the notation is used.

B. Quantum information theory

In this section, we review a few basic definitions and a few theoretical concepts of quantum information that will be used in our paper. We refer the following references [48]–[50] to the reader.

Let $\mathcal{H}$ and $\mathcal{K}$ be finite-dimensional complex Hilbert spaces associated with the input and output quantum systems, respectively. The space of linear operators on $\mathcal{H}$ is denoted $\mathcal{L}(\mathcal{H})$. The state of the quantum system is described by a density operator $\rho \in \mathcal{L}(\mathcal{H})$, which satisfies:

1) **Hermitian**: $\rho^\dagger = \rho$
2) ***Positive semi-definiteness:*** $\rho \geq 0$
3) ***Unit trace:*** $\mathrm{Tr}(\rho) = 1$.

A quantum channel maps quantum states (represented as density operators on a Hilbert space) to other quantum states, accounting for potential noise and decoherence effects. It is a *completely positive, trace-preserving (CPTP) linear map* on the space of density operators.

Definition 1. *(Quantum channel [48]–[50]) A quantum channel is a linear map $\Phi : \mathcal{L}(\mathcal{H}) \longrightarrow \mathcal{L}(\mathcal{K})$ satisfying the following properties:*

1) ***Complete Positivity****: For any $n \in \mathbb{N}$, the map $\Phi \otimes \mathrm{Id}_n : \mathcal{L}(\mathcal{H} \otimes \mathbb{C}^n) \longrightarrow \mathcal{L}(\mathcal{K} \otimes \mathbb{C}^n)$ is positive, where Id_n is the identity map on $\mathbb{C}^n$. That is, for all $X \in \mathcal{L}(\mathcal{H} \otimes \mathbb{C}^n)$ with $X \geq 0$, we have $(\Phi \otimes \mathrm{Id}_n)(X) \geq 0$.*
2) ***Trace Preservation****: For all $\rho \in \mathcal{L}(\mathcal{H})$, $\mathrm{Tr}(\Phi(\rho)) = \mathrm{Tr}(\rho)$.*

Therefore, Φ maps density operators on $\mathcal{H}$ to density operators on $\mathcal{K}$, preserving the physical validity of quantum states.

We will consider finite-dimensional quantum systems with m degrees of freedom, represented by the algebra of $m \times m$ matrices over $\mathbb{C}$, referred to as $\mathbb{M}_m$. The state of a quantum system X is characterized by its density matrix $\rho_X \in \mathbb{M}_m$.

Definition 2. *(von Neumann entropy [48], [49], [51], [52]) The von Neumann entropy of a quantum system X with a density matrix $\rho_X \in \mathbb{M}_m$ is defined as*

$$\mathsf{S}(X) = -\,\mathrm{Tr}(\rho_X \log \rho_X) = -\sum_{1 \leq j \leq m} \lambda_j \log \lambda_j,$$

where $\lambda_1, \dots, \lambda_m$ are the eigenvalues of ρ_X. One way to look at the quantum entropy is as the average amount of qubits needed to describe a system X [51].

The maximum value for $\mathsf{S}(A)$ is given by:

$$\mathsf{S}(X) \leq \log \dim(\mathcal{H}_X) = \log m,$$

where $\mathcal{H}_X$ is the Hilbert space associated with the quantum system X.

Let XY be a bipartite quantum system. Let ρ_{XY} be the density matrix associated to XY resides on the Hilbert space $\mathcal{H}_{XY} = \mathcal{H}_X \otimes \mathcal{H}_Y$. The subsystems X and Y will be represented by the partial traces $\rho_X = \mathrm{Tr}_Y(\rho_{XY})$ and $\rho_Y = \mathrm{Tr}_X(\rho_{XY})$. The von Neumann entropy of a quantum system X conditional on another quantum system Y is defined as (see [45], [48]):

$$\mathsf{S}(X|Y) = \mathsf{S}(XY) - \mathsf{S}(Y),$$

where $\mathsf{S}(XY) = -\mathrm{Tr}(\rho_{XY} \log \rho_{XY})$ is the *joint entropy of* XY and $\mathsf{S}(Y) = -\mathrm{Tr}(\rho_Y \log \rho_Y)$.

The joint entropy of two quantum systems satisfies two important properties:

- **Subadditivity:**
$$\mathsf{S}(XY) \leq \mathsf{S}(X) + \mathsf{S}(Y),$$
- **Araki-Lieb inequality:**
$$\mid \mathsf{S}(X) - \mathsf{S}(Y) \mid \leq \mathsf{S}(XY).$$

The mutual information between two quantum systems X and Y is defined as:

$$I(X:Y) = \mathsf{S}(X) + \mathsf{S}(Y) - \mathsf{S}(XY).$$

Despite many analogies between quantum and classical entropies, they are fundamentally distinct. The conditional von Neumann entropy can be negative, but the conditional classical Shannon entropy is always non-negative.

Definition 3. *(Statistical distance/Total variation distance [53]–[56]). The total variation distance between two random variables X and Y defined on the same sample space $\mathcal{R}$ is defined as*

$$\Delta(X,Y) = \max_{\mathcal{G}\subseteq\mathcal{R}} \Big| \Pr[X \in \mathcal{G}] - \Pr[Y \in \mathcal{G}] \Big| = \frac{1}{2}\left(\sum_{a\in\mathcal{R}} |\Pr[X=a] - \Pr[Y=a]|\right).$$

The analogue of the total variation distance in the quantum setting is the trace distance.

Definition 4. *(Adversarial Pseudometric [20]) For a family $\mathcal{F}$ of quantum circuits that produce a single-bit classical output, the distinguishing advantage of $\mathcal{F}$ between two quantum density matrices ρ and σ of appropriate dimensions is defined as:*

$$\mathsf{Adv}_{\mathcal{F}}(\rho,\sigma) = \max_{C\in\mathcal{F}} \Big| \Pr[C(\rho)=1] - \Pr[C(\sigma)=1] \Big|.$$

The adversarial pseudometric quantifies the maximum probability difference with which any circuit in $\mathcal{F}$ can distinguish between ρ and σ.

Definition 5. *(Trace distance [48], [49], [57]) The trace distance between two density matrices ρ and σ with the same dimensions is defined as*

$$D(\rho,\sigma) = \frac{1}{2}\|\rho - \sigma\|_1.$$

Definition 6. *(Fidelity [48], [49], [58], [59]) Let ρ and σ be two density matrices (quantum states) acting on the same Hilbert space $\mathcal{H}$. Fidelity $F(\rho,\sigma)$ is defined as:*

$$F(\rho,\sigma) = \mathrm{Tr}\left(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right).$$

Lemma 1. *([48]) For any family of quantum circuits $\mathcal{F}$ and two density matrices ρ and σ of the same dimension, the adversarial advantage is bounded by the trace distance*

$$\mathrm{Adv}_{\mathcal{F}}(\rho,\sigma) \leq D(\rho,\sigma).$$

Proof. Consider any quantum circuit $C \in \mathcal{F}$ that performs a measurement on a quantum state and outputs a bit $b \in \{0,1\}$. Any such measurement can be described by a positive operator-valued measure (POVM).

We denote the measurement operators corresponding to output 1 and 0 as E and $(I-E)$, respectively, where $0 \leq E \leq I$ and I is the identity operator on $\mathcal{H}$. The probability that C outputs 1 when measuring ρ is $\Pr[C(\rho)=1] = \mathrm{Tr}(E\rho)$.

Similarly, the probability that C outputs 1 when measuring σ is $\Pr[C(\sigma)=1] = \mathrm{Tr}(E\sigma)$. Then $|\Pr[C(\rho)=1] - \Pr[C(\sigma)=1]| = |\mathrm{Tr}(E(\rho-\sigma))|$. To find the maximum advantage over all circuits in $\mathcal{F}$, we consider the maximal value over all valid measurement operators E. Since $0 \le E \le I$, we have

$$\mathrm{Adv}_{\mathcal{F}}(\rho,\sigma) \le \max_{0\le E\le I} |\mathrm{Tr}(E(\rho-\sigma))|.$$

However, in quantum hypothesis testing, it is known that the maximum of $|\mathrm{Tr}(E(\rho-\sigma))|$ over all $0 \le E \le I$ is equal to the trace distance between ρ and σ. Specifically, from the definition of the trace norm:

$$\|\rho-\sigma\|_1 = \mathrm{Tr}\left[|\rho-\sigma|\right] = 2\max_{0\le E\le I} |\mathrm{Tr}(E(\rho-\sigma))|.$$

Therefore,

$$\max_{0\le E\le I} |\mathrm{Tr}(E(\rho-\sigma))| = \frac{1}{2}\|\rho-\sigma\|_1 = D(\rho,\sigma).$$

and consequently,

$$\mathrm{Adv}_{\mathcal{F}}(\rho,\sigma) \le D(\rho,\sigma).$$

□

Lemma 2. *(The Fuchs–van de Graaf inequalities [48]) The Fuchs–van de Graaf inequalities are given by:*

$$1 - F(\rho,\sigma) \le D(\rho,\sigma) \le \sqrt{1-F(\rho,\sigma)^2}.$$

Let $X \in \mathcal{L}(\mathcal{H})$ be a positive semidefinite operator on a finite-dimensional Hilbert space $\mathcal{H}$. The *support* of X, denoted *supp*(X), is the subspace spanned by all eigenvectors of X with nonzero eigenvalues. Equivalently, if X has spectral decomposition,

$$X = \sum_i \lambda_i |u_i\rangle\langle u_i| \quad (\lambda_i \ge 0),$$

then $supp(X) := span\{|u_i\rangle : \lambda_i > 0\}$.

When we write $(X)^{-1}$ for $X \ge 0$, we always mean the inverse restricted to *supp*(X); that is, we invert only the strictly positive eigenvalues, and vectors in the kernel of X are understood to be outside the domain of $(X)^{-1}$. Such an inverse is sometimes called the *generalized inverse on the support*.

For a linear operator $Y \in \mathcal{L}(\mathcal{H})$ on a finite-dimensional complex Hilbert space $\mathcal{H}$, the *spectral norm* $\|Y\|$ is defined as

$$\|Y\| = \sup_{|\psi\rangle\neq 0, |\psi\rangle\in\mathbb{C}^n} \frac{\|Y|\psi\rangle\|_2}{\||\psi\rangle\|_2},$$

where $\||\psi\rangle\|_2$ is the usual Euclidean norm of the vector $|\psi\rangle$. The spectral norm is equivalent to the largest singular value of A. Formally, if the singular values of A, denoted $\sigma_1, \sigma_2, \ldots, \sigma_n$, are the square roots of the eigenvalues of the positive-semidefinite matrix A^*A (where A^* is the conjugate transpose of A), then:

$$\|A\| = \sigma_{\max} = \sqrt{\lambda_{\max}(A^*A)},$$

where $\lambda_{\max}(A^*A)$ is the largest eigenvalue of A^*A.

Definition 7. *(Quantum Relative Entropy [48]) Given two quantum states ρ and σ, where ρ and σ are density matrices, the quantum relative entropy is defined as*

$$\mathsf{S}(\rho||\sigma) = \begin{cases} Tr\big(\rho(\log\rho - \log\sigma)\big), & \textit{if } supp(\rho) \subseteq supp(\sigma), \\ +\infty, & \textit{otherwise}. \end{cases}$$

Now we will go through some definitions and results, which will be useful to prove the Theorem 9.

Definition 8. *(Moore-Penrose Inverse [60], [61]) Let A be a (real or complex) $m \times n$ matrix. The* Moore-Penrose inverse *of A, denoted A^+, is the unique $n \times m$ matrix satisfying the following four equations called the Penrose equations:*

i) $A\,A^+\,A = A$,
ii) $A^+\,A\,A^+ = A^+$,
iii) $(A\,A^+)^\dagger = A\,A^+$,

iv) $(A^+ A)^\dagger = A^+ A,$

where $X^\dagger$ *denotes the conjugate transpose of* X.

It is well known that for a strictly positive-definite, square, Hermitian matrix M, its Moore-Penrose inverse M^+ is precisely M^{-1}.

Theorem 3. *([60]–[62]) Let* M *be an* $n \times n$ *strictly positive-definite matrix over* $\mathbb{C}$ *or* $\mathbb{R}$*. Then its Moore-Penrose inverse* M^+ *equals the usual inverse* M^{-1}*.*

Proof. For the proof, see [60]. □

Schur complement [60]. Consider a partitioned block matrix $M \in \mathbb{C}^{n\times n}$, structured as:

$$M = \begin{pmatrix} B & C \\ C^\dagger & D \end{pmatrix},$$

where $B \in \mathbb{C}^{k\times k}$, $C \in \mathbb{C}^{k\times(n-k)}$, $D \in \mathbb{C}^{(n-k)\times(n-k)}$.

If D is invertible, the *Schur complement of* D *in* M is defined as:

$$S_D = B - CD^{-1}C^\dagger.$$

If B is invertible, the *Schur complement of* B *in* M is defined as:

$$S_B = D - C^\dagger B^{-1}C.$$

Theorem 4. *(Schur complement condition [60]) A Hermitian matrix* $M \in \mathbb{C}^{n\times n}$ *is positive semi-definite (*$M \geq 0$*) if and only if*

1) *The leading principal submatrix* B *is positive semi-definite:* $B \geq 0$*.*
2) *The Schur complement of* B *in* M*, defined as* $D - C^\dagger B^+ C$*, is positive semi-definite:*

$$D - C^\dagger B^+ C \geq 0,$$

where B^+ *is the Moore-Penrose pseudo-inverse of* B*.*

Corollary 4.1. *(Schur complement condition [60]) If* B *is invertible, the condition simplifies:*

1) ***Positive definiteness of*** B***:*** $B > 0$.
2) ***Positive semi-definiteness of the Schur complement:*** $D - C^\dagger B^{-1} C \geq 0$.

Definition 9. *(Twirling map [63], [64]) Let* $\mathcal{H}$ *be a finite-dimensional Hilbert space, and let* ρ *be a density matrix on* $\mathcal{H}$*, i.e.,*

$$\rho \in \mathcal{D}(\mathcal{H}) = \{\rho \in \mathcal{L}(\mathcal{H}) \mid \rho^\dagger = \rho, \rho \geq 0, \mathrm{Tr}(\rho) = 1\}. \tag{1}$$

Given a unitary representation $U : G \longrightarrow \mathcal{U}(\mathcal{H})$ *of a compact group* G*, the* twirling map *is a quantum channel defined by:*

$$\mathcal{T}_G(\rho) = \int_G U(g)\rho U^\dagger(g)\, d\mu(g), \tag{2}$$

where $d\mu(g)$ *is the* Haar measure *on* G*,* $U(g)$ *is the unitary representation of* $g \in G$*, and the integration is taken over all elements of* G*. The twirling operation averages the state* ρ *over the unitary transformations of the group* G*, producing a state that is invariant under the group* G *[65], [66].*

When G is the symmetric group $\mathrm{Sym(n)}$ and the unitary operators are the permutation matrices, then we can define the twirling map over $\mathrm{Sym}(n)$. We use this definition to compute the expectations later.

Definition 10. *([48]) Let* $\mathcal{H} = (\mathbb{C}^d)^{\otimes n}$ *be the Hilbert space of* n *quantum systems, each of dimension* d*. The symmetric group* $\mathrm{Sym}(n)$ *acts on* $\mathcal{H}$ *via* permutation operators σ_l*, which permute the tensor factors according to* $l \in \mathrm{Sym}(n)$*.*

The twirling operation over $l \in \mathrm{Sym}(n)$ *is defined as:*

$$\mathcal{T}_{\mathrm{Sym}(n)}(\Phi) = \frac{1}{|\,\mathrm{Sym}(n)|} \sum_{l\in\mathrm{Sym}(n)} \sigma_l \Phi \sigma_l^\dagger, \tag{3}$$

where σ_l *is the unitary* permutation operator *corresponding to* $l \in \mathrm{Sym}(n)$*. This operation symmetrizes the density matrix* Φ *with respect to all possible permutations of the subsystems.*

The $\mathrm{Sym}(n)$-twirling map is a completely positive and trace-preserving (CPTP) map that has the following properties:

- **Linear**: For $a, b \in \mathbb{C}$, $\mathcal{T}_{\mathrm{Sym}(n)}(a\rho_1 + b\rho_2) = a\mathcal{T}_{\mathrm{Sym}(n)}(\rho_1) + b\mathcal{T}_{\mathrm{Sym}(n)}(\rho_2)$,
- **Trace-Preserving**: $\mathrm{Tr}(\mathcal{T}_{\mathrm{Sym}(n)}(\rho)) = \mathrm{Tr}(\rho) = 1$.

Quantum one-time pad encryption(QOTP) **[20].** The quantum one-time pad encryption (QOTP) can perfectly hide any quantum message using a random classical key.
The quantum one-time pad encryption scheme is defined by a pair of quantum encryption and decryption circuits $(\mathsf{QOTPEnc}, \mathsf{QOTPDec})$ with

$$\mathsf{QOTPEnc} : (\mathbb{C}^2)^{\otimes n} \times \{0,1\}^{2n} \longrightarrow (\mathbb{C}^2)^{\otimes n} \text{ and } \mathsf{QOTPDec} : (\mathbb{C}^2)^{\otimes n} \times \{0,1\}^{2n} \longrightarrow (\mathbb{C}^2)^{\otimes n}$$

defined as

$$\mathsf{QOTPEnc}(\rho, k) = (X^{k_1} Z^{k_2} \otimes \cdots \otimes X^{k_{2i-1}} Z^{k_{2i}} \otimes \cdots \otimes X^{k_{2n-1}} Z^{k_{2n}})(\rho),$$
$$\mathsf{QOTPDec}(\rho, k) = (Z^{k_1} X^{k_2} \otimes \cdots \otimes Z^{k_{2i-1}} X^{k_{2i}} \otimes \cdots \otimes Z^{k_{2n-1}} X^{k_{2n}})(\rho),$$

for any message $\rho \in (\mathbb{C}^2)^{\otimes n}$ and key $k \in \{0,1\}^{\otimes 2n}$, where X^i, Z^i represent the quantum operation applying the standard Pauli gates X, Z respectively to the i-th qubit.

Lemma 5. *([20], [67]) The quantum one-time pad encryption scheme is correct and perfectly secure for a randomly chosen key. That is,*

$$\mathsf{QOTPDec}(\mathsf{QOTPEnc}(\rho, k), k) = \rho$$

for any key $k \in \{0,1\}^{2n}$, and

$$\sum_{k \in \{0,1\}^{2n}} \frac{1}{2^{2n}} \mathsf{QOTPEnc}(\rho, k) = \sum_{k \in \{0,1\}^{2n}} \frac{1}{2^{2n}} \mathsf{QOTPEnc}(\sigma, k)$$

for any two quantum states $\rho, \sigma \in (\mathbb{C}^2)^{\otimes n}$.

C. Quantum adversarial model

Unless otherwise specified, we consider a quantum computational security setting where the adversaries are quantum polynomial-time (QPT) algorithms. A *QPT adversary* or a *circuit* C means a non-uniform family of circuits $\{C_\lambda\}_{\lambda \in \mathbb{Z}^+}$ with 1-bit classical output, where each circuit has size bounded by $\mathrm{poly}(\lambda)$ and is allowed to use a fixed basis set of gates, for example, $\{\mathsf{H}, \mathsf{CNOT}, \mathsf{S}, \mathsf{T}\}$, etc. Each ancilla qubit is initialized to $|0\rangle$. This model has been studied in quantum secret-sharing and has been studied in [20] for computational quantum secret-sharing.

III. Classical anamorphic encryption

First, we review the original description and definition of anamorphic encryption. Anamorphic encryption is a form of public-key encryption (PKE) that enables a hidden communication mode alongside a regular encryption mode. Specifically, this construction allows a receiver to decrypt a ciphertext to reveal a standard message or, alternatively, a covert message, depending on the use of specific secret keys. Such a scheme can be deployed securely even under coercive environments where a user may be forced to reveal their private key. We refer [11], [12] to the reader for a detailed description.

An anamorphic encryption scheme is defined as a public key encryption scheme $\mathcal{E} = (\mathsf{Gen}, \mathsf{Encrypt}, \mathsf{Decrypt})$, with additional algorithms $\mathcal{A} = (\mathsf{Gen}_a, \mathsf{Encrypt}_a, \mathsf{Decrypt}_a)$ that enable the encryption and decryption of covert messages.

1) **Standard Encryption Scheme:** The PKE scheme $\mathcal{E} = (\mathsf{Gen}, \mathsf{Encrypt}, \mathsf{Decrypt})$ consists of the following algorithms:
   - $\mathsf{Gen}(1^\lambda)$: A key generation algorithm that, given a security parameter λ, outputs a public-private key pair $(\mathsf{pk}, \mathsf{sk})$.
   - $\mathsf{Encrypt}(\mathsf{pk}, m)$: An encryption algorithm that takes a public key pk and a plaintext message m, and outputs a ciphertext c.
   - $\mathsf{Decrypt}(\mathsf{sk}, c)$: A decryption algorithm that takes a private key sk and a ciphertext c, and outputs the original message m or a special symbol $\perp$ if decryption fails.
2) **Anamorphic Triplet:** The anamorphic triplet $\mathcal{A} = (\mathsf{Gen}_a, \mathsf{Encrypt}_a, \mathsf{Decrypt}_a)$ introduces an additional encryption and decryption layer that enables hidden communication:
   - $\mathsf{Gen}_a(1^\lambda)$: Given a security parameter λ, outputs an *anamorphic public key* apk, an *anamorphic secret key* ask, a *double key* dk, and an optional *trapdoor key* tk.
   - $\mathsf{Encrypt}_a(\mathsf{apk}, \mathsf{dk}, m, \hat{m})$: Given the anamorphic public key apk, double key dk, a visible message m, and a covert message $\hat{m}$, it produces an *anamorphic ciphertext* act.
   - $\mathsf{Decrypt}_a(\mathsf{dk}, \mathsf{tk}, \mathsf{ask}, \mathsf{act})$: A decryption algorithm that takes the keys dk, tk, ask, and an anamorphic ciphertext act, outputting the covert message $\hat{m}$ or a special symbol $\perp$ if decryption fails.

To define the security of anamorphic encryption schemes, two games $\mathsf{RealG}_{\mathcal{E}}(\lambda, \mathcal{D})$ and $\mathsf{AnamorphicG}_{\mathcal{A}}(\lambda, \mathcal{D})$ are defined to represent interactions with the real and anamorphic encryption modes, respectively. The goal is to evaluate whether an adversary $\mathcal{D}$ can distinguish between these two games.

In the real game, the encryption scheme operates as a standard PKE scheme without covert capabilities:

1) **Key Generation:** A key pair $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda)$ is generated using the standard key generation function.
2) **Oracle Access:** The adversary $\mathcal{D}$ is provided access to an oracle $\mathcal{O}_\mathsf{E}$ defined by

$$\mathcal{O}_\mathsf{E}(\mathsf{pk}, m, \hat{m}) = \mathsf{Encrypt}(\mathsf{pk}, m),$$

where Encrypt produces a ciphertext containing only m, ignoring any covert message $\hat{m}$.

The adversary $\mathcal{D}$ uses $\mathcal{O}_\mathsf{E}$ to query pairs of messages $(m, \hat{m})$ and receives corresponding ciphertexts generated in a standard encryption mode.

In the anamorphic game, the encryption scheme operates in a mode that embeds a covert channel:

1) **Anamorphic Key Generation:** Anamorphic key generation produces keys $(\mathsf{apk}, \mathsf{ask})$, tk, and dk such that $(\mathsf{apk}, \mathsf{ask}), \mathsf{tk}, \mathsf{dk} \leftarrow \mathsf{Gen}_a(1^\lambda)$.
2) **Oracle Access:** The adversary $\mathcal{D}$ is provided access to an oracle $\mathcal{O}_\mathsf{A}$ defined by

$$\mathcal{O}_\mathsf{A}(\mathsf{apk}, \mathsf{dk}, m, \hat{m}) = \mathsf{Encrypt}_a(\mathsf{apk}, \mathsf{dk}, m, \hat{m}),$$

where $\mathsf{Encrypt}_a$ produces an anamorphic ciphertext that encodes both the visible message m and the covert message $\hat{m}$.

The advantage of an adversary $\mathcal{D}$ in distinguishing between the two games is given by:

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

where $\Pr[\mathsf{RealG}_{\mathcal{E}}(\lambda, \mathcal{D}) = 1]$ is the probability that $\mathcal{D}$ identifies the game as the real game, and $\Pr[\mathsf{AnamorphicG}_{\mathcal{A}}(\lambda, \mathcal{D}) = 1]$ is the probability that $\mathcal{D}$ identifies the game as the anamorphic game.

Definition 11. *(Anamorphic Encryption [11], [12], [27]).*

A PKE scheme $\mathcal{E} = (\mathsf{Gen}, \mathsf{Encrypt}, \mathsf{Decrypt})$ is called an anamorphic encryption scheme if:

1) *It satisfies IND-CPA security (indistinguishability under chosen-plaintext attack).*
2) *There exists an anamorphic triplet $\mathcal{A} = (\mathsf{Gen}_a, \mathsf{Encrypt}_a, \mathsf{Decrypt}_a)$ such that for any probabilistic polynomial-time (PPT) adversary $\mathcal{D}$, the distinguishing advantage $\mathsf{Adv}^{\mathsf{AME}}_{\mathcal{D},\mathcal{E},\mathcal{A}}(\lambda)$ is negligible in λ.*
3) *The existence of a covert message m' remains deniable as the ciphertext c' is indistinguishable from a regular ciphertext.*

In the following section, we introduce an analogue of classical anamorphic encryption within the quantum encryption framework, encompassing both public-key and symmetric-key encryption schemes.

IV. Qauntum Anamorphic Encryption

In this section, we propose an analogous definition of classical anamorphic encryption in the quantum encryption model, where the secrets are quantum density matrices from a finite-dimensional Hilbert space with a quantum polynomial time (QPT) adversary and quantum adversarial pseudometric. In a quantum environment, an anamorphic encryption scheme would need to incorporate quantum-safe encryption methods.

We define a quantum anamorphic encryption scheme as a quantum public key encryption scheme $\mathcal{Q} = (\mathsf{QGen}, \mathsf{QEnc}, \mathsf{QDec})$ with additional algorithms $\mathcal{Q}_a = (\mathsf{QGen}_a, \mathsf{QEnc}_a, \mathsf{QDec}_a)$ to support hidden communication in the presence of quantum adversaries.

A quantum anamorphic encryption scheme is a quantum public-key encryption (QPKE) scheme with an additional anamorphic triplet of quantum algorithms, enabling hidden messages within ciphertexts. We denote this quantum anamorphic encryption scheme by the tuple $\mathcal{Q} = (\mathsf{QGen}, \mathsf{QEnc}, \mathsf{QDec})$ and $\mathcal{Q}_a = (\mathsf{QGen}_a, \mathsf{QEnc}_a, \mathsf{QDec}_a)$, where:

1) **Quantum Public Key Encryption Scheme**: The QPKE scheme $\mathcal{Q} = (\mathsf{QGen}, \mathsf{QEnc}, \mathsf{QDec})$ consists of:
   - $\mathsf{QGen}(1^\lambda)$: A key generation algorithm that takes a security parameter λ and outputs a public-private key pair $(\mathsf{qpk}, \mathsf{qsk})$.
   - $\mathsf{QEnc}(\mathsf{qpk}, \rho)$: A quantum encryption algorithm that takes a public key qpk and a quantum state ρ representing a message, producing a ciphertext in a quantum state qc.
   - $\mathsf{QDec}(\mathsf{qsk}, \mathsf{qc})$: A quantum decryption algorithm that takes a private key qsk and a ciphertext qc, outputting the original message ρ or a special failure symbol $\perp$ if decryption fails.
2) **Quantum Anamorphic Triplet**: The anamorphic triplet $\mathcal{Q}_a = (\mathsf{QGen}_a, \mathsf{QEnc}_a, \mathsf{QDec}_a)$ introduces additional quantum algorithms to enable covert communication:

- $\mathsf{QGen}_a(1^\lambda)$: An anamorphic key generation algorithm that, given a security parameter λ, outputs an anamorphic public key qapk, an anamorphic secret key qask, a double key qdk, and a potentially empty trapdoor key qtk.
- $\mathsf{QEnc}_a(\mathsf{qapk}, \mathsf{qdk}, \rho, \hat{\rho})$: An anamorphic encryption algorithm that, given qapk, qdk, a visible message state ρ, and a covert message state $\hat{\rho}$, outputs an anamorphic ciphertext qact.
- $\mathsf{QDec}_a(\mathsf{qdk}, \mathsf{qtk}, \mathsf{qask}, \mathsf{qact})$: An anamorphic decryption algorithm that takes the double key qdk, trapdoor key qtk, anamorphic secret key qask, and anamorphic ciphertext qact, and outputs the covert message $\hat{\rho}$ or a failure symbol $\perp$.

To evaluate the security of quantum anamorphic encryption schemes, we introduce two games that distinguish the quantum real and anamorphic encryption modes. These games, $\mathsf{RealG}_{\mathcal{Q}}(\lambda, \mathcal{D})$ and $\mathsf{AnamorphicG}_{\mathcal{Q}_a}(\lambda, \mathcal{D})$, consider adversaries in the quantum polynomial-time (QPT) model.

In the real game, the encryption scheme operates in a traditional QPKE setting with no covert channel.

1) **Key Generation:** The key pair $(\mathsf{qpk}, \mathsf{qsk}) \leftarrow \mathsf{QGen}(1^\lambda)$ is generated using the standard quantum key generation function.
2) **Oracle Access:** The adversary $\mathcal{D}$ is provided access to a quantum oracle $\mathcal{O}_{\mathsf{E}}$ defined by:
$$\mathcal{O}_{\mathsf{E}}(\mathsf{qpk}, \rho, \hat{\rho}) = \mathsf{QEnc}(\mathsf{qpk}, \rho),$$
where QEnc produces a ciphertext containing only the visible message ρ, ignoring any covert message $\hat{\rho}$.

The adversary $\mathcal{D}$ interacts with $\mathcal{O}_{\mathsf{E}}$, querying pairs of quantum states $(\rho, \hat{\rho})$ and receiving quantum ciphertexts generated in the standard encryption mode.

In the anamorphic game, the encryption scheme operates in an anamorphic mode that enables covert communication.

1) **Anamorphic Key Generation:** The anamorphic key generation algorithm produces $(\mathsf{qapk}, \mathsf{qask})$, qtk, and qdk, such that $(\mathsf{qapk}, \mathsf{qask}), \mathsf{qtk}, \mathsf{qdk} \leftarrow \mathsf{QGen}_a(1^\lambda)$.
2) **Oracle Access:** The adversary $\mathcal{D}$ is provided access to a quantum oracle $\mathcal{O}_{\mathsf{A}}$ defined by:
$$\mathcal{O}_{\mathsf{A}}(\mathsf{qapk}, \mathsf{qdk}, \rho, \hat{\rho}) = \mathsf{QEnc}_a(\mathsf{qapk}, \mathsf{qdk}, \rho, \hat{\rho}),$$
where QEnc_a produces an anamorphic ciphertext encoding both the visible message ρ and the covert message $\hat{\rho}$.

The adversary $\mathcal{D}$ uses $\mathcal{O}_{\mathsf{A}}$ to query quantum states $(\rho, \hat{\rho})$, receiving anamorphic ciphertexts that contain both visible and covert components.

To quantify the advantage of a quantum adversary in computationally distinguishing between the two games, we define the distinguishing advantage with respect to a family of quantum circuits $\mathcal{F}$:
$$\mathsf{Adv}_{\mathcal{F}}^{\mathsf{AME}}(\rho, \sigma) = \max_{C \in \mathcal{F}} \left| \Pr\left[C(\rho) = 1\right] - \Pr\left[C(\sigma) = 1\right] \right|,$$
where C is a circuit from $\mathcal{F}$ that outputs 1 if it identifies the quantum state as belonging to the anamorphic game [20].

Next, we define the quantum analogue of anamorphic encryption.

Definition 12. *A QPKE scheme* $\mathcal{Q} = (\mathsf{QGen}, \mathsf{QEnc}, \mathsf{QDec})$ *is defined as a quantum anamorphic encryption scheme if:*

1) *It satisfies quantum IND-CPA security (indistinguishability under chosen-plaintext attack with quantum adversaries).*
2) *There exists a quantum anamorphic triplet* $\mathcal{Q}_a = (\mathsf{QGen}_a, \mathsf{QEnc}_a, \mathsf{QDec}_a)$ *such that, for any quantum polynomial-time (QPT) adversary* $\mathcal{D}$*, the computationally distinguishing advantage*
$$\mathsf{Adv}_{\mathcal{D}}^{\mathsf{AME}}(\lambda) = \left| \Pr\left[\mathsf{RealG}_{\mathcal{Q}}(\lambda, \mathcal{D}) = 1\right] - \Pr\left[\mathsf{AnamorphicG}_{\mathcal{Q}_a}(\lambda, \mathcal{D}) = 1\right] \right| < \mathsf{negl}(\lambda).$$

The above definition of quantum anamorphic encryption, which we have discussed, is based on public key encryption. Now we propose an analogous definition of quantum anamorphic encryption based on symmetric key encryption.

A general quantum symmetric key encryption is defined as follows:

Definition 13. *A quantum symmetric-key encryption scheme is a triplet of quantum algorithms*$(\mathsf{QKGen}, \mathsf{QEnc}, \mathsf{QDec})$*, where:*

- $\mathsf{QKGen}(1^\lambda)$*: Takes as input a security parameter* 1^λ *and outputs a secret key* k*. The key* k *can be classical or quantum.*
- $\mathsf{QEnc}(k, \rho)$*: Takes the secret key* k *and a quantum message state* ρ *in some Hilbert space* $\mathcal{H}$*, and outputs a ciphertext* qc *a quantum state in some, possibly different, Hilbert space* $\mathcal{H}_c$*.*
- $\mathsf{QDec}(k, \mathsf{qc})$*: Takes the secret key* k *and a ciphertext state* qc*, and attempts to recover the original message* ρ*. If the ciphertext is invalid, it outputs* $\perp$*.*

Now, we propose a definition of quantum anamorphic encryption. A *quantum anamorphic encryption scheme* adds a second *anamorphic* mode of operation, consisting of another triplet of quantum algorithms $(\mathsf{QKGen}_a, \mathsf{QEnc}_a, \mathsf{QDec}_a)$ which allows *embedding* a covert message $\hat{\rho}$ inside the same ciphertext structure, but in such a way that an adversary cannot distinguish between normal encryption and anamorphic encryption with high probability, where:

- **Anamorphic Key Generation** ($\mathsf{QKGen_a}$)**:** The algorithm $\mathsf{QKGen_a}$ takes as input the security parameter 1^λ and returns $k_a = (k, \mathsf{dk}, \mathsf{tk})$, where k_a is the *anamorphic secret key* when the system is operating in *anamorphic mode*. The key k is the normal key used to encrypt the original message, and the dk double key and tk trapdoor key are additional secret keys that can be classical keys or quantum states that may be necessary to embed and extract covert messages and which will never be given to the dictator. Either might be an empty string if not needed.
- **Anamorphic Encryption (**QEnc_a**):** The algorithm QEnc_a takes as input the key k_a and two quantum messages ρ, the original and $\hat{\rho}$, the covert quantum message, and returns a quantum anamorphic ciphertext qact, that is, $\mathsf{QEnc}_a\big(k_a, \rho, \hat{\rho}\big) = \mathsf{qact}$, which must be indistinguishable from a original ciphertext produced by $(k, \rho) \mapsto \mathsf{QEnc}(k, \rho)$.
- **Anamorphic Decryption (**$\mathsf{QDec_a}$**):** The algorithm takes as input the anamorphic key k_a and anamorphic ciphertext qact and outputs the covert message $\hat{\rho}$, that is, $\mathsf{QDec}_a\big(k_a, \mathsf{qact}\big) = \hat{\rho}$. If recovery fails, the algorithm outputs $\perp$.

Security definition via two indistinguishability games: We define two worlds or games as previous, a *real* (no covert channel) world and an *anamorphic* (with covert channel) world. An adversary attempts to distinguish these two scenarios.

The Real Game ($\mathsf{RealG_Q}(\lambda, \mathcal{D})$):

1) A secret key $k \leftarrow \mathsf{QKGen}(1^\lambda)$ is generated, which is the normal encryption key.
2) The adversary $\mathcal{D}$ is given oracle access to a real encryption map

$$\mathcal{O}_{\mathsf{E}}(k, \rho, \hat{\rho}) \;=\; \mathsf{QEnc}\big(k, \rho\big),$$

which *ignores* the covert message $\hat{\rho}$, that is, the oracle only encrypts the original state ρ in the normal mode.
3) $\mathcal{D}$ can make polynomially many queries and eventually outputs a guess bit $b \in \{0, 1\}$, meaning it guesses whether it is in the real or anamorphic game.

The Anamorphic Game ($\mathsf{AnamorphicG}_{\mathsf{Q}_a}(\lambda, \mathcal{D})$):

1) The anamorphic keys are generated: $k_a \leftarrow \mathsf{QKGen}_a(1^\lambda)$.
2) The adversary $\mathcal{D}$ is given oracle access to

$$\mathcal{O}_{\mathsf{A}}\big(k_a, \rho, \hat{\rho}\big) \;=\; \mathsf{QEnc}_a\big(k_a, \rho, \hat{\rho}\big),$$

which produces an *anamorphic ciphertext* that contains both ρ and $\hat{\rho}$.
3) As before, $\mathcal{D}$ makes a number of queries and finally outputs a guess bit $b \in \{0, 1\}$.

Adversarial Advantage. We define the advantage of adversary $\mathcal{D}$ distinguishing the above two games by

$$\mathsf{Adv}^{\mathsf{AME}}_{\mathcal{D},\mathsf{Q},\mathsf{Q}_a}(\lambda) \;=\; \Big|\Pr\big[\mathsf{RealG_Q}(\lambda, \mathcal{D}) = 1\big] \;-\; \Pr\big[\mathsf{AnamorphicG}_{\mathsf{Q}_a}(\lambda, \mathcal{D}) = 1\big]\Big|.$$

Definition 14. *(Quantum Anamorphic Symmetric-Key Encryption) A triple* $(\mathsf{QKGen}, \mathsf{QEnc}, \mathsf{QDec})$ *is called a* quantum symmetric-key encryption scheme*, and a triple* $(\mathsf{QKGen}_a, \mathsf{QEnc}_a, \mathsf{QDec}_a)$ *is called its* anamorphic extension*, if:*

1) ***Correctness.*** *For all original and covert quantum messages, ρ and $\hat{\rho}$, respectively,*

$$\mathsf{QDec}\big(k,\, \mathsf{QEnc}(k, \rho)\big) \;=\; \rho$$

and similarly,

$$\mathsf{QDec}_a\big(k_a,\, \mathsf{QEnc}_a(k_a, \rho, \hat{\rho})\big) \;=\; \hat{\rho}.$$

2) ***Security Against Chosen-Plaintext (Quantum) Attacks.*** *The scheme* $(\mathsf{QKGen}, \mathsf{QEnc}, \mathsf{QDec})$ *is* quantum-IND-CPA secure *(in the symmetric-key sense), meaning that no QPT adversary $\mathcal{D}$ can distinguish encryptions of two chosen quantum states (or classical messages) with more than negligible advantage in λ.*
3) ***Anamorphic Indistinguishability.*** *There is an anamorphic extension* $(\mathsf{QKGen}_a, \mathsf{QEnc}_a, \mathsf{QDec}_a)$ *such that for every QPT adversary $\mathcal{D}$, the distinguishing advantage*

$$\mathsf{Adv}^{\mathsf{AME}}_{\mathcal{D},\mathsf{Q},\mathsf{Q}_a}(\lambda) \;=\; \big|\Pr\big[\mathsf{RealG_Q}(\lambda, \mathcal{D}) = 1\big] \;-\; \Pr\big[\mathsf{AnamorphicG}_{\mathsf{Q}_a}(\lambda, \mathcal{D}) = 1\big]\big| \;<\; \mathsf{negl}(\lambda).$$

In other words, the ciphertexts generated by QEnc *versus those generated by* QEnc_a *(even on* pairs *of inputs* $(\rho, \hat{\rho})$*) are computationally indistinguishable to any quantum adversary.*

V. Technical Details

In this section, we have proposed a construction of quantum anamorphic symmetric key encryption. Let $M_o \in (\mathbb{C}^2)^{\otimes d_1}$ be the mixed density matrix representing the original message, and let $M_c \in (\mathbb{C}^2)^{\otimes d_2}$ be the mixed density matrix representing the covert message. Hence both the matrices M_o and M_c are Hermitian, positive semi-definite with $\mathrm{Tr}(M_o) = 1$ and $\mathrm{Tr}(M_c) = 1$. But as per our construction, we restrict the density matrix M_o to be strictly positive definite. The anamorphic message contains both the original and covert messages, which Alice needs to send to Bob. On the dictator's demand, Bob will hand over only the anamorphic ciphertext and the original keys to the dictator so that the dictator gets only the original message, and also he will be unable to distinguish between the original and the anamorphic ciphertexts.

A. *Main Construction*

We independently encrypt M_o and M_c using the QOTP scheme, with separate keys k and k', respectively.

1) **Encryption of M_o:** Let $M_o' = \mathsf{QOTPEnc}(M_o, k)$, where $\mathsf{QOTPEnc}$ denotes the QOTP encryption operator with key $k \in \{0,1\}^{2d_1}$. This operation is defined as follows:

$$M_o' = \left(X^{k_1} Z^{k_2} \otimes X^{k_3} Z^{k_4} \otimes \cdots \otimes X^{k_{2d_1-1}} Z^{k_{2d_1}}\right) M_o \left(X^{k_1} Z^{k_2} \otimes X^{k_3} Z^{k_4} \otimes \cdots \otimes X^{k_{2d_1-1}} Z^{k_{2d_1}}\right)^\dagger. \tag{4}$$

2) **Encryption of M_c:** Let $M_c' = \mathsf{QOTPEnc}(M_c, k')$, where $k' \in \{0,1\}^{2d_2}$ is the QOTP key used for encrypting M_c. This operation is defined as:

$$M_c' = \left(X^{k_1'} Z^{k_2'} \otimes X^{k_3'} Z^{k_4'} \otimes \cdots \otimes X^{k_{2d_2-1}'} Z^{k_{2d_2}'}\right) M_c \left(X^{k_1'} Z^{k_2'} \otimes X^{k_3'} Z^{k_4'} \otimes \cdots \otimes X^{k_{2d_2-1}'} Z^{k_{2d_2}'}\right)^\dagger. \tag{5}$$

We define the Hilbert spaces associated with M_o' and M_c' by $\mathcal{H}_o = (\mathbb{C}^2)^{\otimes d_1}$ which is of dimension 2^{d_1} denotes the space for the original message and $\mathcal{H}_c = (\mathbb{C}^2)^{\otimes d_2}$ which is of the dimension 2^{d_2}, denotes the covert message space, respectively.

Without loss of generality, let $d_2 \leq d_1$ and if $d_2 < d_1$, then pad the density matrix M_c' with $(2^{d_1} - 2^{d_2})$ zero rows and columns to make it a $(2^{d_1} \times 2^{d_1})$ matrix, and we denote it by M_c''.

We construct M_c'' by introducing $(d_1 - d_2)$ *ancillary qubits* in a fixed state $|0\rangle^{\otimes(d_1-d_2)}$.

Define the extended Hilbert space

$$\mathcal{H}_c \otimes (\mathbb{C}^2)^{\otimes(d_1-d_2)} \cong \left(\mathbb{C}^2\right)^{\otimes d_1} = \mathcal{H}_c^e.$$

Consider the isometric embedding

$$V : \mathcal{H}_c \longrightarrow \mathcal{H}_c^e$$

defined by

$$V|\psi\rangle = |\psi\rangle \otimes |0\rangle^{\otimes(d_1-d_2)}, \quad \forall |\psi\rangle \in \mathcal{H}_c.$$

Here, $|0\rangle$ denotes the computational-basis state of a single qubit.
For a density matrix $M_c' \in \mathcal{L}(\mathcal{H}_c)$, define

$$M_c'' = V M_c' V^\dagger \in \mathcal{L}(\mathcal{H}_c^e).$$

We typically describe transformations on density operators by completely positive, trace-preserving (CPTP) maps. The above padding can be described as a linear map

$$\mathcal{E}^{\mathrm{pad}} : \mathcal{L}(\mathcal{H}_c) \longrightarrow \mathcal{L}(\mathcal{H}_c^e).$$

We define

$$\mathcal{E}^{\mathrm{pad}}(M_c') = M_c'' = \begin{cases} M_c', & \text{if } d_1 = d_2, \\ V M_c' V^\dagger, & \text{if } d_2 < d_1, \end{cases} \tag{6}$$

where V is the isometric embedding from above. Since $V^\dagger V = I_{\mathcal{H}_c}$ and $V V^\dagger$ is the projector onto $\mathcal{H}_c \otimes |0\rangle^{\otimes(d_1-d_2)}$, $\mathcal{E}^{\mathrm{pad}}$ is completely positive and trace-preserving. Since V is an isometry,

- **Positivity is preserved:** For any $\phi \in \mathcal{H}_c^e$,

$$\langle\phi| V M_c' V^\dagger |\phi\rangle \geq 0.$$

- **Trace is preserved:**

$$\mathrm{Tr}\big(V M_c' V^\dagger\big) = \mathrm{Tr}(M_c'), \quad (\text{since} \quad V^\dagger V = I_{\mathcal{H}_c}).$$

Hence, it is a valid quantum channel.

Given the security parameter $\mathsf{negl}(\lambda) > 0$, choose $\eta \in \mathbb{Z}^+$ such that $\dfrac{1}{\eta} < \mathsf{negl}(\lambda)$ and

$$\frac{1}{\eta^2}\left\|(M_c'')^\dagger (M_o')^{-1} M_c''\right\| \;\leq\; \frac{1}{4}\lambda_{\min}(M_o'), \tag{7}$$

where $\lambda_{\min}(M_o')$ is the minimum eigenvalue of M_o' on its support and $\|\cdot\|$ is the operator norm. As η is a non-zero real number, it is clear that the matrix M_o' should be not only positive semi-definite but also strictly positive definite, and hence the matrix M_o should be strictly positive definite for our construction. In our construction, we construct a state M_a in a larger Hilbert space $(\mathbb{C}^2)^{\otimes(d_1+1)}$.

We define

$$\begin{aligned} M_a &:= |0\rangle\langle 0| \otimes \tfrac{1}{2}\, M_o' \;+\; |0\rangle\langle 1| \otimes \tfrac{1}{\eta}\, M_c'' \;+\; |1\rangle\langle 0| \otimes \tfrac{1}{\eta}\left(M_c''\right)^\dagger \;+\; |1\rangle\langle 1| \otimes \tfrac{1}{2}\, M_o' \qquad (8)\\ &= \begin{pmatrix} \frac{1}{2}M_o' & \frac{1}{\eta}M_c'' \\ \frac{1}{\eta}(M_c'')^\dagger & \frac{1}{2}M_o' \end{pmatrix}. \qquad (9)\end{aligned}$$

For $b \in \{0,1\}$, we define

$$\begin{aligned} M_a^{(b)} &:= (1-b)\Big(\,|0\rangle\langle 0| \otimes \tfrac{1}{2}\, M_o' \;+\; |1\rangle\langle 1| \otimes \tfrac{1}{2}\, M_o'\Big) \;+\; bM_a \qquad (10)\\ &= (1-b)\begin{pmatrix} \frac{1}{2}M_o' & \mathbf{0}_{2^{d_1}\times 2^{d_1}} \\ \mathbf{0}_{2^{d_1}\times 2^{d_1}} & \frac{1}{2}M_o' \end{pmatrix} + bM_a. \qquad (11)\end{aligned}$$

To construct the final state for encoding, we choose a permutation matrix σ_l of order $(2^{d_1+1} \times 2^{d_1+1})$ uniformly randomly and create the final state

$$M_f^{(b)} := \sigma_l M_a^{(b)} \sigma_l^\dagger. \tag{12}$$

Note that the state $M_f^{(0)}$ is the *original ciphertext*; as before, applying the permutation matrix, it is only encrypted using the original key and can be decrypted using only the original key.

We now describe the quantum anamorphic decryption to extract the original message.
Define

$$M_d^{(1)} \;:=\; \sigma_l^\dagger\, M_f^{(1)}\, \sigma_l. \tag{13}$$

Since σ_l is a permutation matrix, it is unitary, and $\sigma_l^\dagger = \sigma_l^{-1}$. Hence $M_d^{(1)}$ recovers the block structure used by the encryption. We define the following projectors on the first qubit:

$$\Pi_0 \;=\; |0\rangle\langle 0| \,\otimes\, I_{2^{d_1}}, \qquad \Pi_1 \;=\; |1\rangle\langle 1| \,\otimes\, I_{2^{d_1}}, \tag{14}$$

where $I_{2^{d_1}}$ is the identity operator on $\mathcal{H}_o$. Then

$$\Pi_0 + \Pi_1 \;=\; I_{2^{d_1+1}}, \quad \Pi_0\,\Pi_1 \;=\; 0, \quad \Pi_0^2 = \Pi_0, \quad \Pi_1^2 = \Pi_1. \tag{15}$$

Define

$$M_d^{(1)}(0,0) \;=\; \Pi_0\, M_d^{(1)}\, \Pi_0 \quad \text{in} \quad (\mathbb{C}^2)^{\otimes(d_1+1)}, \tag{16}$$

and

$$M_d^{(1)}(1,1) \;=\; \Pi_1\, M_d^{(1)}\, \Pi_1 \quad \text{in} \quad (\mathbb{C}^2)^{\otimes(d_1+1)}. \tag{17}$$

By *extracting* these two blocks (first and fourth) and *adding* them, we obtain an operator on $(\mathbb{C}^2)^{\otimes(d_1+1)}$ (since $\Pi_0+\Pi_1 = I_{2^{d_1+1}}$ on the first qubit, restricted to the appropriate blocks).
We get

$$M_a^{(0)} \;=\; M_d^{(1)}(0,0) \;+\; M_d^{(1)}(1,1) \;=\; \big(|0\rangle\langle 0| \otimes I_{2^{d_1}}\big)\, M_d^{(1)}\, \big(|0\rangle\langle 0| \otimes I_{2^{d_1}}\big) \;+\; \big(|1\rangle\langle 1| \otimes I_{2^{d_1}}\big)\, M_d^{(1)}\, \big(|1\rangle\langle 1| \otimes I_{2^{d_1}}\big). \tag{18}$$

Now to extract $(0,0)$-block and $(1,1)$-block, that is the first block and the fourth block only, in the reduced space $\mathcal{H}_o$, we define

$$\begin{aligned} \widetilde{M}_o'(0,0)\Big|_{\mathcal{H}_o} &:= \left(\langle 0| \otimes I_{2^{d_1}}\right) M_a^{(0)} \left(|0\rangle \otimes I_{2^{d_1}}\right), \qquad (19)\\ \widetilde{M}_o'(1,1)\Big|_{\mathcal{H}_o} &:= \left(\langle 1| \otimes I_{2^{d_1}}\right) M_a^{(0)} \left(|1\rangle \otimes I_{2^{d_1}}\right). \qquad (20)\end{aligned}$$

Then, $M'_o := \widetilde{M}'_o(0,0)\Big|_{\mathcal{H}_o} + \widetilde{M}'_o(1,1)\Big|_{\mathcal{H}_o}$, since each block represents half of the total contribution,

$$\frac{1}{2}M'_o + \frac{1}{2}M'_o = M'_o. \tag{21}$$

Recall the QOTP decryption operation $\mathsf{QOTPDec}(\cdot, k) : \mathcal{L}(\mathcal{H}_o) \longrightarrow \mathcal{L}(\mathcal{H}_o)$. For a key $k = (k_1, k_2, \ldots, k_{2d_1-1}, k_{2d_1})$, the corresponding QOTP *encryption* is given by

$$\mathsf{QOTPEnc}(M_o, k) \;=\; \Big(\bigotimes_{j=1}^{d_1} X^{k_{2j-1}}\, Z^{k_{2j}}\Big)\, M_o\, \Big(\bigotimes_{j=1}^{d_1} X^{k_{2j-1}}\, Z^{k_{2j}}\Big)^{\dagger}. \tag{22}$$

Hence, $\mathsf{QOTPDec}(\cdot, k)$ applies the adjoint of that unitary factor

$$\mathsf{QOTPDec}(M', k) \;=\; \Big(\bigotimes_{j=1}^{d_1} X^{k_{2j-1}}\, Z^{k_{2j}}\Big)^{\dagger}\, M'\, \Big(\bigotimes_{j=1}^{d_1} X^{k_{2j-1}}\, Z^{k_{2j}}\Big). \tag{23}$$

Accordingly, our final normal decryption for the original state is

$$M_o \;=\; \mathsf{QOTPDec}\big(M'_o,\, k\big) \;=\; \Big(\bigotimes_{j=1}^{d_1} X^{k_{2j-1}} Z^{k_{2j}}\Big)^{\dagger}\, M'_o\, \Big(\bigotimes_{j=1}^{d_1} X^{k_{2j-1}} Z^{k_{2j}}\Big). \tag{24}$$

The output is precisely the original density matrix M_o, completing the decryption for the original message.

Next, we describe the extraction and decryption of the covert message. After computing $\sigma_l^{\dagger} M_f^{(1)} \sigma_l$, the *second* block or the *third* block of $M_d^{(1)}$ corresponds to $\frac{1}{\eta}\, M''_c$ or its adjoint.

Define the partial extraction operators

$$\Pi_{0,1}(X) = (|0\rangle\langle 0| \otimes I_{2^{d_1}})\,(X)\,(|1\rangle\langle 1| \otimes I_{2^{d_1}})\,,$$
$$\Pi_{1,0}(X) = (|1\rangle\langle 1| \otimes I_{2^{d_1}})\,(X)\,(|0\rangle\langle 0| \otimes I_{2^{d_1}})\,.$$

Applying the partial operators to $M_d^{(1)}$, we get

$$M_d^{(1)}(0,1) \;= \Pi_{0,1}(M_d^{(1)}) = \;\big(|0\rangle\langle 0| \otimes I_{2^{d_1}}\big)\, M_d^{(1)}\, \big(|1\rangle\langle 1| \otimes I_{2^{d_1}}\big) \quad \text{in} \quad (\mathbb{C}^2)^{\otimes(d_1+1)} \tag{25}$$

and

$$M_d^{(1)}(1,0) \;= \Pi_{1,0}(M_d^{(1)}) = \;\big(|1\rangle\langle 1| \otimes I_{2^{d_1}}\big)\, M_d^{(1)}\, \big(|0\rangle\langle 0| \otimes I_{2^{d_1}}\big) \quad \text{in} \quad (\mathbb{C}^2)^{\otimes(d_1+1)}. \tag{26}$$

Now we reduce to the Hilbert space $\mathcal{H}_c^e$ to extract the covert block

$$M_{\text{covert}}(0,1)\big|_{\mathcal{H}_c^e} = (\langle 0| \otimes I_{2^{d_1}})\, M_d^{(1)}\, (|1\rangle \otimes I_{2^{d_1}})\,, \tag{27}$$

$$M_{\text{covert}}(1,0)\big|_{\mathcal{H}_c^e} = (\langle 1| \otimes I_{2^{d_1}})\, M_d^{(1)}\, (|0\rangle \otimes I_{2^{d_1}})\,. \tag{28}$$

We may choose either of these blocks and denote it by $M_{\text{covert}} \in \mathcal{L}((\mathbb{C}^2)^{\otimes d_1})$.
Recall that, at encryption, the covert block had a factor of $\frac{1}{\eta}$. Hence, to recover the padded covert operator M''_c, we define

$$\widetilde{M''_c} \;:=\; \eta\, M_{\text{covert}}. \tag{29}$$

If $M_{\text{covert}} = \frac{1}{\eta}\, M''_c$, then $\widetilde{M''_c} = M''_c$; or if $M_{\text{covert}} = \frac{1}{\eta}\,(M''_c)^{\dagger}$, then $\widetilde{M''_c} = (M''_c)^{\dagger}$.
Recall that $\widetilde{M''_c} \in \mathcal{L}\big(\mathcal{H}_c^e\big)$, but the original message belongs in $\mathcal{H}_c$. To recover an operator in $\mathcal{L}(\mathcal{H}_c)$, we *unembed* via the adjoint of V.

Define

$$\widetilde{M'_c} \;:=\; V^{\dagger}\, \widetilde{M''_c}\, V \;\in\; \mathcal{L}\big(\mathcal{H}_c\big). \tag{30}$$

If $\widetilde{M''_c} = M''_c$, we get $\widetilde{M'_c} = M'_c$. In particular, since $V^{\dagger}$ removes the zero-padding (the last $(2^{d_1} - 2^{d_2})$ rows and columns), $\widetilde{M'_c}$ is the recovered padded covert operator in the original dimension $2^{d_2} \times 2^{d_2}$.

The QOTP *decryption* for key $k' = (k'_1, k'_2, \ldots, k'_{2d_2-1}, k'_{2d_2})$ is:

$$\mathsf{QOTPDec}\big(M',\, k'\big) \;=\; \Big(\bigotimes_{j=1}^{d_2} X^{k'_{2j-1}}\, Z^{k'_{2j}}\Big)^{\dagger}\, M'\, \Big(\bigotimes_{j=1}^{d_2} X^{k'_{2j-1}}\, Z^{k'_{2j}}\Big). \tag{31}$$

Hence the covert user obtains

$$M_c \;=\; \mathsf{QOTPDec}\big(\widetilde{M}_c',\, k'\big) \;=\; \Big(\bigotimes_{j=1}^{d_2} X^{k'_{2j-1}}\, Z^{k'_{2j}}\Big)^{\dagger}\; \widetilde{M}_c'\; \Big(\bigotimes_{j=1}^{d_2} X^{k'_{2j-1}}\, Z^{k'_{2j}}\Big). \tag{32}$$

This final output is the *covert* density operator M_c originally encrypted.

The quantum anamorphic encryption algorithm is described below:

Algorithm 1 Quantum Anamorphic Encryption(QAE)

Input: Original density matrix M_o, covert density matrix M_c, dimensions d_1, d_2 ($d_2 \leq d_1$), security parameter $\eta \in \mathbb{Z}^+$, and permutation matrix σ_l.

Output: Anamorphic quantum state $M_f^{(1)}$.

Steps:

1. Sample keys:

Draw key $k \leftarrow \{0,1\}^{2d_1}$ uniformly at random.

Draw key $k' \leftarrow \{0,1\}^{2d_2}$ uniformly at random.

2. Encrypt M_o using QOTP:

Compute $M_o' = \mathsf{QOTPEnc}(M_o, k)$ as:

$$M_o' = \left(X^{k_1} Z^{k_2} \otimes \cdots \otimes X^{k_{2d_1-1}} Z^{k_{2d_1}}\right) M_o \left(X^{k_1} Z^{k_2} \otimes \cdots \otimes X^{k_{2d_1-1}} Z^{k_{2d_1}}\right)^{\dagger}.$$

3. Encrypt M_c using QOTP:

Compute $M_c' = \mathsf{QOTPEnc}(M_c, k')$ as:

$$M_c' = \left(X^{k_1'} Z^{k_2'} \otimes \cdots \otimes X^{k'_{2d_2-1}} Z^{k'_{2d_2}}\right) M_c \left(X^{k_1'} Z^{k_2'} \otimes \cdots \otimes X^{k'_{2d_2-1}} Z^{k'_{2d_2}}\right)^{\dagger}.$$

4. Pad M_c':

If $d_2 < d_1$, extend M_c' to $M_c'' \in \mathcal{L}((\mathbb{C}^2)^{\otimes d_1})$ using the isometric embedding:

$$V : \mathcal{H}_c \to \mathcal{H}_c \otimes (\mathbb{C}^2)^{\otimes(d_1-d_2)},$$

defined as:

$$V|\psi\rangle = |\psi\rangle \otimes |0\rangle^{\otimes(d_1-d_2)}, \quad \forall|\psi\rangle \in \mathcal{H}_c.$$

The padded matrix is:

$$M_c'' = V M_c' V^{\dagger}.$$

5. Construct M_a:

Define the anamorphic quantum state:

$$M_a = |0\rangle\langle 0| \otimes \tfrac{1}{2}\, M_o' \;+\; |0\rangle\langle 1| \otimes \tfrac{1}{\eta}\, M_c'' \;+\; |1\rangle\langle 0| \otimes \tfrac{1}{\eta}\left(M_c''\right)^{\dagger} \;+\; |1\rangle\langle 1| \otimes \tfrac{1}{2}\, M_o'.$$

6. Apply permutation σ_l:

Construct the final anamorphic quantum state:

$$M_f^{(1)} = \sigma_l M_a \sigma_l^{\dagger},$$

where σ_l is a uniformly random permutation matrix of size $2^{d_1+1} \times 2^{d_1+1}$.

7. Return $M_f^{(1)}$:

Output $M_f^{(1)}$ as the encrypted anamorphic quantum state.

Now we describe the decryption algorithm to extract and decrypt the original secret from the anamorphic ciphertext:

Algorithm 2 Decryption of Original Secret from Anamorphic Ciphertext(DOM)

Input: Anamorphic state $M_f^{(1)} \in \mathcal{L}((\mathbb{C}^2)^{\otimes(d_1+1)})$, permutation matrix P_l, QOTP key $k \in \{0,1\}^{2d_1}$, dimension d_1.

Output: Original density matrix M_o.

Steps:

1. Apply the inverse permutation:

Compute the intermediate state $M_d^{(1)}$ by applying the inverse of σ_l:

$$M_d^{(1)} = \sigma_l^\dagger M_f^{(1)} \sigma_l.$$

2. Extract the first block and fourth block:

Define the projectors:

$$\Pi_0 = |0\rangle\langle 0| \otimes I_{2^{d_1}}, \qquad \Pi_1 = |1\rangle\langle 1| \otimes I_{2^{d_1}},$$

where $I_{2^{d_1}}$ is the identity operator on $\mathcal{H}_o = (\mathbb{C}^2)^{\otimes d_1}$.

Extract the blocks:

$$M_d^{(1)}(0,0) = \Pi_0 M_d^{(1)} \Pi_0, \qquad M_d^{(1)}(1,1) = \Pi_1 M_d^{(1)} \Pi_1.$$

Combine the blocks to obtain the quantum state:

$$M_a^{(0)} = M_d^{(1)}(0,0) + M_d^{(1)}(1,1).$$

3. Reduce the extracted blocks to the smaller space $\mathcal{H}_o$:

$$\widetilde{M}_o'(0,0) := (\langle 0| \otimes I_{2^{d_1}})\, M_a^{(0)}\, (|0\rangle \otimes I_{2^{d_1}}),$$
$$\widetilde{M}_o'(1,1) := (\langle 1| \otimes I_{2^{d_1}})\, M_a^{(0)}\, (|1\rangle \otimes I_{2^{d_1}}).$$

4. Combine the reduced blocks:

$$M_o' := \widetilde{M}_o'(0,0) + \widetilde{M}_o'(1,1).$$

Since each block represents half of the total contribution,

$$M_o' = \frac{1}{2}M_o' + \frac{1}{2}M_o' = M_o'.$$

5. Apply QOTP decryption:

Use the QOTP decryption key $k = (k_1, k_2, \ldots, k_{2d_1})$ to recover M_o:

$$M_o = \mathsf{QOTPDec}(M_o', k) = \Big(\bigotimes_{j=1}^{d_1} X^{k_{2j-1}} Z^{k_{2j}}\Big)^\dagger M_o' \Big(\bigotimes_{j=1}^{d_1} X^{k_{2j-1}} Z^{k_{2j}}\Big).$$

6. Return the original density matrix M_o:

Output M_o, completing the decryption.

The covert secret extraction and decryption algorithm from the anamorphic ciphertext, is described below:

Algorithm 3 Decryption of Covert Message from Anamorphic Ciphertext(DCM)

Input: Anamorphic state $M_f^{(1)} \in \mathcal{L}((\mathbb{C}^2)^{\otimes(d_1+1)})$, permutation matrix σ_l, QOTP key $k' \in \{0,1\}^{2d_2}$, dimensions d_1, d_2, and scaling factor $\eta \in \mathbb{Z}^+$.

Output: Covert density matrix $M_c \in \mathcal{L}((\mathbb{C}^2)^{\otimes d_2})$.

Steps:

1. Apply the inverse permutation:

Compute the intermediate state $M_d^{(1)}$ by applying the inverse of P_l:

$$M_d^{(1)} = \sigma_l^\dagger M_f^{(1)} \sigma_l.$$

2. Extract one of the off-diagonal blocks (second or third):

By construction, one covert block resides in the $|0\rangle\langle 1|$-subspace and the other in the $|1\rangle\langle 0|$-subspace. Define the partial extraction operators:

$$\Pi_{0,1}(X) = (|0\rangle\langle 0| \otimes I_{2^{d_1}})\,(X)\,(|1\rangle\langle 1| \otimes I_{2^{d_1}}),$$
$$\Pi_{1,0}(X) = (|1\rangle\langle 1| \otimes I_{2^{d_1}})\,(X)\,(|0\rangle\langle 0| \otimes I_{2^{d_1}}).$$

Apply the above operators to extract the blocks:

$$M_d^{(1)}(0,1) = \Pi_{0,1}(M_d^{(1)}),$$
$$M_d^{(1)}(1,0) = \Pi_{1,0}(M_d^{(1)}).$$

Reduce to the smaller Hilbert space:

$$M_{\text{covert}}(0,1)\big|_{\mathcal{H}_c^e} = (\langle 0| \otimes I_{2^{d_1}})\, M_d^{(1)}\, (|1\rangle \otimes I_{2^{d_1}}),$$
$$M_{\text{covert}}(1,0)\big|_{\mathcal{H}_c^e} = (\langle 1| \otimes I_{2^{d_1}})\, M_d^{(1)}\, (|0\rangle \otimes I_{2^{d_1}}).$$

Assign the covert block:

$$M_{\text{covert}} = \begin{cases} M_{\text{covert}}(0,1)\big|_{\mathcal{H}_c^e}, & \text{if we choose the second block as covert block} \\ M_{\text{covert}}(1,0)\big|_{\mathcal{H}_c^e}, & \text{if we choose the third block as covert block} \end{cases}$$

3. Multiply by η:

Recover the padded covert operator:

$$\widetilde{M}_c'' = \eta\, M_{\text{covert}}.$$

4. Remove the zero-padding:

Use the isometric embedding $V : \mathcal{H}_c \to \mathcal{H}_c^e$, with adjoint $V^\dagger$, to unembed:

$$\widetilde{M}_c' = V^\dagger \widetilde{M}_c'' V.$$

The result $\widetilde{M}_c' \in \mathcal{L}((\mathbb{C}^2)^{\otimes d_2})$ is the padded covert density operator.

5. Apply QOTP decryption:

Use the QOTP key $k' = (k_1', k_2', \ldots, k_{2d_2}')$ to recover M_c:

$$M_c = \mathsf{QOTPDec}(\widetilde{M}_c', k') = \Big(\bigotimes_{j=1}^{d_2} X^{k_{2j-1}'} Z^{k_{2j}'}\Big)^\dagger \widetilde{M}_c' \Big(\bigotimes_{j=1}^{d_2} X^{k_{2j-1}'} Z^{k_{2j}'}\Big).$$

6. Return the covert density matrix M_c:

Output M_c, completing the covert decryption procedure.

Next, we describe an algorithm to extract the original ciphertext from the anamorphic ciphertext, which we will use in the definition of anamorphic secret-sharing.

Algorithm 4 Extraction of Original Ciphertext from Anamorphic Ciphertext(EOC)

Input: Anamorphic state $M_f^{(1)} \in \mathcal{L}((\mathbb{C}^2)^{\otimes(d_1+1)})$, permutation matrix σ_l, QOTP key $k \in \{0,1\}^{2d_1}$, dimension d_1.
Output: Original ciphertext $M_f^{(0)}$.
Steps:
1. Apply the inverse permutation:
Compute the intermediate state $M_d^{(1)}$ by applying the inverse of σ_l:

$$M_d^{(1)} = \sigma_l^\dagger M_f^{(1)} \sigma_l.$$

2. Extract the first block and fourth block:
Define the projectors:

$$\Pi_0 = |0\rangle \langle 0| \otimes I_{2^{d_1}}, \qquad \Pi_1 = |1\rangle \langle 1| \otimes I_{2^{d_1}},$$

where $I_{2^{d_1}}$ is the identity operator on $\mathcal{H}_o = (\mathbb{C}^2)^{\otimes d_1}$.
Extract the blocks:

$$M_d^{(1)}(0,0) = \Pi_0 M_d^{(1)} \Pi_0, \qquad M_d^{(1)}(1,1) = \Pi_1 M_d^{(1)} \Pi_1.$$

Combine the blocks to obtain the quantum state:

$$M_a^{(0)} = M_d^{(1)}(0,0) + M_d^{(1)}(1,1).$$

3. Extract the original ciphertext:
Apply the permutation matrix σ_l to recover the original ciphertext:

$$M_f^{(0)} = \sigma_l M_a^{(0)} \sigma_l^\dagger.$$

4. Return the original ciphertext $M_f^{(0)}$:
Output $M_f^{(0)}$, completing the extraction.

Remark 1. *The algorithm* DOM *can be applied to the original ciphertext $M_f^{(0)}$ too. Exactly in a similar way, we can retrieve the original message M_o from $M_f^{(0)}$.*

Now we discuss the following theorems and corollaries to prove the Theorem 9 and the corollary 9.1.

Definition 15. *(Rayleigh Quotient [Section 4.2, Page 176, [60]]) Let A be a Hermitian operator on an n-dimensional complex Hilbert space $\mathcal{H}$. The Rayleigh quotient $R(A;x)$ associated with $x \neq 0$ is defined as*

$$R(A;x) \;=\; \frac{x^* A x}{x^* x}. \tag{33}$$

We now recall the fundamental *variational characterization* of eigenvalues of a Hermitian operator. This is sometimes called the *Rayleigh–Ritz theorem* (in finite dimensions).

Theorem 6. *(Variational Characterization of the Extreme Eigenvalues [60], [68], [69]) Let A be a Hermitian $n \times n$ matrix (or Hermitian operator on an n-dimensional space). Denote its eigenvalues by*

$$\lambda_1(A) \;\leq\; \lambda_2(A) \;\leq\; \cdots \;\leq\; \lambda_n(A) \tag{34}$$

ordered in a nondecreasing sequence. Then

$$\min_{|v\rangle \neq 0} R(A;|v\rangle) \;=\; \lambda_1(A), \quad \max_{|v\rangle \neq 0} R(A;|v\rangle) \;=\; \lambda_n(A). \tag{35}$$

In particular,

$$\lambda_{\min}(A) \;=\; \min_{\||v\rangle\|_2 = 1} \langle v| A |v\rangle, \quad \lambda_{\max}(A) \;=\; \max_{\||v\rangle\|_2 = 1} \langle v| A |v\rangle. \tag{36}$$

The following Corollary 6.1 can easily be derived from the Theorem 6, which we have used in our proof of the Theorem 9. The Lemma 8 is also easy to prove using basic linear algebra, and we have used it to prove Corollary 8.1. We have included them for completeness.

Corollary 6.1. *Let $X, Y \geq 0$ be positive semi-definite matrices on the same finite-dimensional Hilbert space $\mathcal{H}$. If*

$$\lambda_{\max}(Y) \;\;\leq\;\; \lambda_{\min}(X), \tag{37}$$

then

$$(X - Y) \ \geq \ 0. \tag{38}$$

Proof. Since $X, Y \geq 0$, all their eigenvalues are nonnegative. To show that $X - Y$ is positive semi-definite, we show that for all $|v\rangle \in \mathcal{H}$,

$$\langle v| \, (X - Y) \, |v\rangle \ \geq \ 0. \tag{39}$$

As $\lambda_{\min}(X)$ is the smallest eigenvalue of X, and by the variational characterization of eigenvalues (or Rayleigh quotients), we have

$$\frac{\langle v| \, X \, |v\rangle}{\| \, |v\rangle \, \|_2^2} \ \geq \ \lambda_{\min}(X). \tag{40}$$

Since $X \geq 0$, for any $|v\rangle \neq 0$,

$$\langle v| \, X \, |v\rangle \ \geq \ \lambda_{\min}(X) \, \| \, |v\rangle \, \|_2^2. \tag{41}$$

Since $\lambda_{\max}(Y)$ is the largest eigenvalue of Y, the Rayleigh quotient satisfies

$$\frac{\langle v| \, Y \, |v\rangle}{\| \, |v\rangle \, \|_2^2} \ \leq \ \lambda_{\max}(Y). \tag{42}$$

Similarly, for $Y \geq 0$, we have

$$\langle v| \, Y \, |v\rangle \ \leq \ \lambda_{\max}(Y) \, \| \, |v\rangle \, \|_2^2. \tag{43}$$

Combining both the equations together, we get that, for any nonzero $|v\rangle \in \mathcal{H}$,

$$\langle v| \, X \, |v\rangle \ - \ \langle v| \, Y \, |v\rangle \ \geq \ \left(\lambda_{\min}(X) \, \| \, |v\rangle \, \|_2^2\right) \ - \ \left(\lambda_{\max}(Y) \, \| \, |v\rangle \, \|_2^2\right) \ = \ \Big(\lambda_{\min}(X) - \lambda_{\max}(Y)\Big) \, \| \, |v\rangle \, \|_2^2. \tag{44}$$

By our assumption, $(\lambda_{\min}(X) - \lambda_{\max}(Y)) \geq 0$.
Therefore,

$$\forall \, |v\rangle \in \mathcal{H}, \quad \langle v| \, (X - Y) \, |v\rangle \ \geq \ \Big(\lambda_{\min}(X) - \lambda_{\max}(Y)\Big) \, \| \, |v\rangle \, \|_2^2 \ \geq \ 0. \tag{45}$$

Hence, $(X - Y) \geq 0$, that is, $(X - Y)$ is a positive semi-definite matrix. ☐

Lemma 7. *([60]) Let $X \geq 0$ be a Hermitian and positive semi-definite matrix. Then*

$$\lambda_{\max}(X) \ = \ \|X\|, \tag{46}$$

where $\lambda_{\max}(M)$ is the largest eigenvalue of M, and $\|M\|$ is the spectral norm or operator norm of X.

In general, if A and B are two positive semi-definite matrices, then AB may not be a positive semi-definite matrix unless commutativity holds, that is $AB = BA$. But in our case we next prove that if M_o' is strictly positive definite and M_c'' is positive semi-definite, then the matrix $M_c'' \, (M_o')^{-1} \, M_c''$ is also positive semi-definite. Here we note that it is *not* necessary that the matrix M_c'' should be strictly positive definite.

Lemma 8. *Let $Y \in M_n(\mathbb{C})$ be a Hermitian positive definite matrix, and let $X \in M_n(\mathbb{C})$ be a Hermitian positive semi-definite matrix. Then*

$$XY^{-1}X \quad \textit{is a Hermitian positive semi-definite matrix.}$$

Moreover, $XY^{-1}X$ is strictly positive definite if and only if X is invertible.

Proof. For vectors $v, w \in \mathbb{C}^n$, we define, $\langle v, w\rangle := v^\dagger w$. Then $\langle \cdot, \cdot \rangle$ defines an inner product on $\mathbb{C}^n$. Now as X is positive semi-definite, for all non-zero vectors $v \in \mathbb{C}^n$, $\langle v, Xv\rangle \geq 0$. Since Y is positive definite, its inverse Y^{-1} exists and is also positive definite. The matrix $XY^{-1}X$ is Hermitian since both X and Y are Hermitian.

Consider an arbitrary vector $v \in \mathbb{C}^n$ and also consider the inner product $\langle v, XY^{-1}Xv\rangle$.
Define $w := Xv$. Then $\langle v, XY^{-1}Xv\rangle = \langle w, Y^{-1}w\rangle$. Since Y, is positive definite, for all $w \in \mathbb{C}^n$, $\langle w, Y^{-1}w\rangle \geq 0$. Therefore, $XY^{-1}X$ is also a positive semi- definite matrix.

Note that $XY^{-1}X$ fails to be strictly positive definite precisely if there exists a nonzero vector v such that

$$\langle v, \, XY^{-1}Xv\rangle \ = \ 0. \tag{47}$$

However, we have

$$\langle v, \, XY^{-1}Xv\rangle \ = \ \langle Xv, \, Y^{-1}Xv\rangle. \tag{48}$$

Since Y^{-1} is strictly positive definite, $\langle w, Y^{-1}w\rangle = 0$ if and only if $w = 0$. Hence,

$$\langle Xv, Y^{-1}Xv\rangle = 0 \quad \text{iff} \quad Xv = 0. \tag{49}$$

Thus, if X has a nontrivial kernel, there is a nonzero v with $Xv = 0$, leading to $\langle v, XY^{-1}Xv\rangle = 0$. This shows that if X is not invertible, then $XY^{-1}X$ is not strictly positive definite.

Conversely, if X is invertible, then $Xv = 0$ implies $v = 0$. Hence the only way $\langle v, XY^{-1}Xv\rangle = 0$ can hold is if $v = 0$.

Therefore, $XY^{-1}X$ is always Hermitian and positive semi-definite. It is strictly positive definite if and only if X is invertible. □

Corollary 8.1. *The matrix $M''_c(M'_o)^{-1}M''_c$ is a Hermitian and a positive semi-definite matrix.*

Proof. By applying the Lemma 8. with $X = M''_c$ and $Y = M'_o$, the result follows. □

We now state one of the main theorems of our paper.

Theorem 9. *Given a security parameter $\mathsf{negl}(\lambda) > 0$, with $\eta \in \mathbb{Z}^+$ such that $\frac{1}{\eta} < \mathsf{negl}(\lambda)$ both the original and the anamorphic quantum states $M_f^{(0)}$ and $M_f^{(1)}$ are quantum density matrices, if*

$$\frac{1}{\eta^2}\,\|(M''_c)^\dagger\,(M'_o)^{-1}\,M''_c\| \;\le\; \frac{1}{4}\,\lambda_{\min}(M'_o), \tag{50}$$

where $\lambda_{\min}(M'_o)$ is the minimum eigenvalue of M'_o on its support and $\|\cdot\|$ is the operator norm and M'_o is a strictly positive definite matrix.

Proof. We consider both the block matrices

$$M_a^{(0)} \;=\; \begin{pmatrix} \frac{1}{2}M'_o & \mathbf{0}_{2^{d_1}\times 2^{d_1}} \\ \mathbf{0}_{2^{d_1}\times 2^{d_1}} & \frac{1}{2}M'_o \end{pmatrix} \text{ and } M_a^{(1)} \;=\; \begin{pmatrix} \frac{1}{2}\,M'_o & \frac{1}{\eta}\,M''_c \\ \frac{1}{\eta}\left(M''_c\right)^\dagger & \frac{1}{2}\,M'_o \end{pmatrix}, \tag{51}$$

where $M'_o \in \mathcal{L}(\mathcal{H}_o)$ is the QOTP-encrypted version of a density matrix M_o. Since QOTP preserves positivity and trace, $M'_o \ge 0$ and $\mathrm{Tr}(M'_o) = 1$. Therefore, the matrix $M_a^{(0)}$ is a density matrix.

The encrypted covert matrix $M''_c \in \mathcal{L}(\mathcal{H}_c^e)$ is another operator obtained by encrypting the covert message M_c using QOTP and then padding the encrypted covert message M'_c. Since the matrix M_c is also a density matrix, and since QOTP preserves positivity and trace, $M'_c \ge 0$ and $\mathrm{Tr}(M'_c) = 1$. As $\mathcal{E}^{\mathrm{pad}}(M'_c) \;=\; V\,M'_c\,V^\dagger = M''_c$, and $\mathcal{E}^{\mathrm{pad}}$ is an isometry and completely positive by construction of V, $M''_c \ge 0$ and $\mathrm{Tr}(M''_c) = 1$. As M_c is Hermitian, M'_c is also Hermitian, and consequently M''_c is also Hermitian. The parameter $\eta > 0$ is used to scale the off-diagonal blocks. It is clear that $\mathrm{Tr}(M_a) = 1$. Therefore, we only analyze whether M_a is a positive semi-definite $(M_a \ge 0)$ matrix. Writing

$$M_a \;=\; \begin{pmatrix} A & B \\ B^\dagger & A \end{pmatrix}, \quad \text{where} \quad A \;=\; \tfrac{1}{2}\,M'_o, \quad B \;=\; \tfrac{1}{\eta}\,M''_c, \tag{52}$$

we note that

$$A = \tfrac{1}{2}\,M'_o \;\ge\; 0 \quad \text{iff} \quad M'_o \;\ge\; 0, \tag{53}$$

which is true by hypothesis. The potential problem for positivity arises from the off-diagonal blocks B and $B^\dagger$.
By the Schur complement condition 4 for the positivity of a 2×2 block matrix, is that

$$A \;\ge\; 0, \quad \text{and} \quad A - B\,A^+\,B^\dagger \;\ge\; 0 \quad , \tag{54}$$

where A^+ denotes the generalized Moore Penrose inverse on the *supp*(A). By the Theorem 3. We have $(M'_o)^+ = (M'_o)^{-1}$. Substituting $A = \frac{1}{2}\,M'_o$ and $B = \frac{1}{\eta}\,M''_c$, we obtain

$$\tfrac{1}{2}\,M'_o \;-\; \left(\tfrac{1}{\eta}\,M''_c\right)\left(\tfrac{1}{2}\,M'_o\right)^{-1}\left(\tfrac{1}{\eta}\,M''_c\right)^\dagger \;\ge\; 0 \quad \text{iff} \quad \tfrac{1}{2}\,M'_o \;-\; \tfrac{1}{\eta^2}\,(M''_c)\left(\tfrac{1}{2}\,M'_o\right)^{-1}(M''_c)^\dagger \;\ge\; 0. \tag{55}$$

We prove that a sufficient condition is to require

$$\frac{1}{\eta^2}\,\|(M''_c)^\dagger\,(M'_o)^{-1}\,M''_c\| \;\le\; \frac{1}{4}\,\lambda_{\min}(M'_o), \tag{56}$$

where $\lambda_{\min}(M'_o)$ is the minimum eigenvalue of M'_o on its support and $\|\cdot\|$ is the operator norm. Since $A = \frac{1}{2}\,M'_o$, and $M'_o \ge 0$ is invertible on its support, we can write

$$A^{-1} \;=\; \left(\tfrac{1}{2}\,M'_o\right)^{-1} = 2\left(M'_o\right)^{-1} \quad \text{on } \mathit{supp}(M'_o). \tag{57}$$

Let $B = \frac{1}{\eta}\, M_c''$. Then $B^\dagger = \frac{1}{\eta}\,(M_c'')^\dagger = \frac{1}{\eta}\, M_c''$ (since $M_c'' \geq 0$, and M_c'' is also Hermitian).
Hence,

$$B^\dagger\, A^{-1}\, B = \left(\tfrac{1}{\eta}\, M_c''\right) \left(2\,(M_o')^{-1}\right) \left(\tfrac{1}{\eta}\, M_c''\right) = \tfrac{2}{\eta^2}\, M_c''\,(M_o')^{-1}\, M_c''. \tag{58}$$

Thus,

$$A - B^\dagger A^{-1} B = \tfrac{1}{2}\, M_o' \;-\; \tfrac{2}{\eta^2}\, M_c''\,(M_o')^{-1}\, M_c''. \tag{59}$$

To ensure

$$\tfrac{1}{2}\, M_o' \;-\; \tfrac{2}{\eta^2}\, M_c''\,(M_o')^{-1}\, M_c'' \;\;\geq\; 0, \tag{60}$$

we show that a sufficient condition, is that the largest eigenvalue of $\frac{2}{\eta^2}\, M_c''\,(M_o')^{-1}\, M_c''$ *does not exceed* the smallest eigenvalue of $\frac{1}{2}\, M_o'$.

Let

$$X \;=\; \tfrac{1}{2}\, M_o', \quad Y \;=\; \tfrac{2}{\eta^2}\, M_c''\,(M_o')^{-1}\, M_c''. \tag{61}$$

We want $(X - Y) \geq 0$. We know that if X, Y are positive semi-definite, then

$$\lambda_{\max}(Y) \;\leq\; \lambda_{\min}(X) \quad \text{implies} \quad (X - Y) \;\geq 0, \tag{62}$$

where $\lambda_{\max}$ and $\lambda_{\min}$ denote the maximum and minimum eigenvalues on the relevant support.

Now,

$$\lambda_{\min}(X) = \lambda_{\min}\left(\tfrac{1}{2}\, M_o'\right) = \tfrac{1}{2}\, \lambda_{\min}(M_o'), \tag{63}$$

since scaling an operator by $\frac{1}{2}$ scales all eigenvalues by $\frac{1}{2}$,

and

$$\lambda_{\max}(Y) \;=\; \lambda_{\max}\left(\tfrac{2}{\eta^2}\, M_c''\,(M_o')^{-1}\, M_c''\right) = \tfrac{2}{\eta^2}\, \lambda_{\max}\left(M_c''\,(M_o')^{-1}\, M_c''\right). \tag{64}$$

Because $M_c'', (M_o')^{-1}$, are positive semi-definite and positive definite, respectively, by the Corollary 8.1, $M_c''\,(M_o')^{-1}\, M_c''$ is positive semi-definite, and by Lemma 7, we get $\lambda_{\max}\big(M_c''\,(M_o')^{-1}\, M_c''\big) \;=\; \|(M_c'')^\dagger\,(M_o')^{-1}\, M_c''\|$, i.e. the spectral norm of that product.

Therefore, we need

$$\tfrac{2}{\eta^2}\, \lambda_{\max}\big(M_c''\,(M_o')^{-1}\, M_c''\big) \;\;\leq\;\; \tfrac{1}{2}\, \lambda_{\min}(M_o'), \tag{65}$$

which is equivalent to

$$\frac{1}{\eta^2}\, \lambda_{\max}\big(M_c''\,(M_o')^{-1}\, M_c''\big) \;\;\leq\;\; \frac{1}{4}\, \lambda_{\min}(M_o'). \tag{66}$$

Therefore,

$$\frac{1}{\eta^2}\, \big\|\,(M_c'')^\dagger\,(M_o')^{-1}\, M_c''\big\| \;\;\leq\;\; \frac{1}{4}\, \lambda_{\min}(M_o'). \tag{67}$$

This condition forces $M_a \geq 0$. Since M_o' is a density operator, $\lambda_{\min}(M_o') \geq 0$. By making η sufficiently large, one can always satisfy $\frac{1}{\eta^2}\;\|(M_c'')^\dagger\,(M_o')^{-1}\, M_c''\| \;\;\leq\;\; \frac{1}{4}\, \lambda_{\min}(M_o')$. Since the permutation matrices are unitary matrices, they preserve the positive semi-definiteness and unit trace. Hence, both the matrices $M_f^{(0)}$ and $M_f^{(1)}$ are positive semi-definite with unit trace. Therefore, both the original and anamorphic matrices are quantum density matrices. □

Corollary 9.1. *(A weaker sufficient condition) Given a security parameter* $\mathsf{negl}(\lambda) > 0$*, with* $\eta \in \mathbb{Z}^+$ *such that* $\dfrac{1}{\eta} < \mathsf{negl}(\lambda)$ *both the original and the anamorphic quantum states* $M_f^{(0)}$ *and* $M_f^{(1)}$ *are quantum density matrices, if*

$$\frac{2\lambda_{\max}(M_c'')}{\lambda_{\min}(M_o')} \leq \eta, \tag{68}$$

where $\lambda_{\min}(M_o')$ *and* $\lambda_{\max}(M_c'')$ *are the minimum and maximum eigenvalues of* M_o' *and* M_c'' *on their respective supports.*

Proof. If

$$\frac{\lambda_{\max}(M_c'')}{\eta} \;\leq\; \frac{1}{2}\, \lambda_{\min}(M_o'), \tag{69}$$

then,

$$\frac{\lambda_{\max}(M_c'')}{\eta} \;\leq\; \frac{1}{2}\,\lambda_{\min}(M_o') \quad \text{implies} \quad \frac{1}{\eta^2}\,\frac{\lambda_{\max}(M_c'')^2}{\lambda_{\min}(M_o')} \;\leq\; \frac{1}{4}\,\lambda_{\min}(M_o'). \tag{70}$$

We know that for any two matrices A and B of compatible dimensions, $\|AB\| \;\leq\; \|A\|\,\|B\|$. Therefore, we get,

$$\|(M_c'')^\dagger\,(M_o')^{-1}\,M_c''\| \;\leq\; \|(M_c'')^\dagger\|\,\|(M_o')^{-1}\|\,\|M_c''\|. \tag{71}$$

Since M_c'' is positive semi-definite and Hermitian, $(M_c'')^\dagger = M_c''$ and hence $\|(M_c'')^\dagger\| = \|M_c''\|$.

Therefore,

$$\|(M_c'')^\dagger\,(M_o')^{-1}\,M_c''\| \;\leq\; \|M_c''\|^2\,\|(M_o')^{-1}\|. \tag{72}$$

Since M_c'' is positive semi-definite, all its eigenvalues are non-negative, and the spectral norm equals the maximum eigenvalue 7,

$$\|M_c''\| = \lambda_{\max}(M_c''). \tag{73}$$

Similarly, since M_o' is strictly positive-definite, $\lambda_{\min}(M_o') > 0$ and hence,

$$\|(M_o')^{-1}\| = \lambda_{\max}\big((M_o')^{-1}\big) = \frac{1}{\lambda_{\min}(M_o')}. \tag{74}$$

Combining the equations 72,73,74, we get,

$$\|(M_c'')^\dagger\,(M_o')^{-1}\,M_c''\| \;\leq\; \frac{\lambda_{\max}(M_c'')^2}{\lambda_{\min}(M_o')}. \tag{75}$$

Hence,

$$\frac{1}{\eta^2}\,\|(M_c'')^\dagger\,(M_o')^{-1}\,M_c''\| \leq \frac{1}{\eta^2}\,\frac{\lambda_{\max}(M_c'')^2}{\lambda_{\min}(M_o')} \leq \frac{1}{4}\,\lambda_{\min}(M_o'), \tag{76}$$

which satisfies the sufficient condition we proved in Theorem 9. □

- **Adversary's Observations in the Two Games**

i) **The real game RealG**$_{\mathcal{Q}}(\lambda, \mathcal{D})$: In the real game, only the original message M_o is encrypted and sent. We have the encrypted message $M_o' = U_k M_o U_k^\dagger$ by the QOTP and the key k. Then we have constructed the following message $M_a^{(0)} = \begin{pmatrix} \frac{1}{2}M_o' & \mathbf{0}_{2^{d_1}\times 2^{d_1}} \\ \mathbf{0}_{2^{d_1}\times 2^{d_1}} & \frac{1}{2}M_o' \end{pmatrix}$. The final state we have is $M_f^{(0)} = \sigma_l M_a^{(0)} \sigma_l^\dagger$.

ii) **The anamorphic game AnamorphicG**$_{\mathcal{Q}_a}(\lambda, \mathcal{D})$ In the anamorphic game, both M_o and M_c are encrypted and sent. The encrypted message is $M_o' = U_k M_o U_k^\dagger, \quad M_c' = U_{k'} M_c U_{k'}^\dagger$. Then we have combined both the original message and the hidden message as $M_a^{(1)} = M_a$. Finally, we have constructed the state $M_f^{(1)} = \sigma_l M_a^{(1)} \sigma_l^\dagger$.

In both games, the adversary receives the state $M_f^{(b)}$ for $b \in \{0,1\}$, without knowledge of l, k, k', d_1, d_2, η. The expectation $\mathbb{E}_l[M_f^{(0)}]$ and $\mathbb{E}_l[M_f^{(1)}]$ represent the average state the adversary would get if they sampled many ciphertexts using random keys.

Theorem 10. *The expectations of the original and the anamorphic states are*

$$\mathbb{E}_{l,d_1,k}[M_f^{(0)}] = \frac{1}{2^{d_1+1}} I_{2^{d_1+1}}, \tag{77}$$

where $I_{2^{d_1+1}}$ is the identity matrix of dimension 2^{d_1+1} and after considering expectation $\mathbb{E}_k[M_o']$ and $\mathbb{E}_{k'}[M_c'']$ separately we get,

$$\mathbb{E}_l\big[M_f^{(1)}\big] = \alpha\big(M_a^{(1)}\big)\,I + \beta\big(M_a^{(1)}\big)\,J = \frac{2^{d_1+1} - 1 - \frac{2}{\eta}}{2^{d_1+1}(2^{d_1+1}-1)} I \;+\; \frac{2/\eta}{2^{d_1+1}(2^{d_1+1}-1)} J, \tag{78}$$

where the matrix J is such that $J_{i,j} = 1$ for all $i, j \in [2^{d_1+1}]$.
Hence the trace distance between the expectations is

$$D(\mathbb{E}_l[M_f^{(1)}], \mathbb{E}_l[M_f^{(0)}]) = \frac{1}{\eta\, 2^{d_1}} \tag{79}$$

which is less than $\mathsf{negl}(\lambda)$,
and

$$D(\mathbb{E}_l[M_f^{(1)}], \mathbb{E}_l[M_f^{(1)'}]) = 0. \tag{80}$$

for any two density matrices $M_f^{(1)}$ and $M_f^{(1)'}$, when the randomization is taken over two different keys l, d_1, d_2, k, k', η and $\tilde{l}, \tilde{d_1}, \tilde{d_2}, \tilde{k}, \tilde{k'}, \tilde{\eta}$ from the same set $\mathrm{Sym}(n) \times [2^{d_1+1}] \times [2^{d_1+1}] \times \{0,1\}^{d_1} \times \{0,1\}^{d_2} \times \mathcal{J}$, with uniform distribution.

Proof. We recall that the Quantum One-Time Pad (QOTP) encryption of an n-qubit state ρ with key $k \in \{0,1\}^{2n}$ is given by $\mathsf{QOTPEnc}(\rho, k) = U_k \rho U_k^\dagger$, where $U_k = \bigotimes_{i=1}^n X^{k_{2i-1}} Z^{k_{2i}}$. The expectation over all possible keys k is

$$\mathbb{E}_k[\mathsf{QOTPEnc}(\rho, k)] = \frac{1}{2^{2n}} \sum_{k \in \{0,1\}^{2n}} U_k \rho U_k^\dagger = \frac{I_{2^n}}{2^n} \operatorname{Tr}(\rho) = \frac{I_{2^n}}{2^n}, \tag{81}$$

since $\operatorname{Tr}(\rho) = 1$.

Let $M_o \in (\mathbb{C}^2)^{\otimes d_1}$ be an arbitrary d_1-qubit state (density matrix) representing the original matrix. The QOTP encryption of M_o with key $k \in \{0,1\}^{2d_1}$ is $M_o' = U_k M_o U_k^\dagger$.

We compute the expectation over all keys k,

$$\mathbb{E}_k[M_o'] = \frac{1}{2^{2d_1}} \sum_{k \in \{0,1\}^{2d_1}} U_k M_o U_k^\dagger. \tag{82}$$

Using the properties of Pauli operators and the fact that the set $\{U_k\}_{k \in \{0,1\}^{2d_1}}$ forms an orthonormal basis for operators on $(\mathbb{C}^2)^{\otimes d_1}$ (up to normalization), we can express M_o in terms of Pauli operators

$$M_o = \sum_{P \in \mathcal{P}} c_P P, \tag{83}$$

where the sum is over all d_1-qubit Pauli operators P, and $c_P = \frac{1}{2^{d_1}} \operatorname{Tr}(P M_o)$. Then, we have

$$\mathbb{E}_k[M_o'] = \frac{1}{2^{2d_1}} \sum_{k \in \{0,1\}^{2d_1}} U_k \left(\sum_{P \in \mathcal{P}} c_P P \right) U_k^\dagger = \sum_{P \in \mathcal{P}} c_P \left(\frac{1}{2^{2d_1}} \sum_{k \in \{0,1\}^{2d_1}} U_k P U_k^\dagger \right). \tag{84}$$

Note that for any Pauli operator P (excluding the identity), we have $\frac{1}{2^{2d_1}} \sum_{k \in \{0,1\}^{2d_1}} U_k P U_k^\dagger = 0$. This is because the conjugation of P by U_k effectively randomizes P over all possible Pauli operators, and their average is zero unless P is the identity operator, and for $P = I$, we have $\frac{1}{2^{2d_1}} \sum_{k \in \{0,1\}^{2d_1}} U_k I U_k^\dagger = I$. Therefore, $\mathbb{E}_k[M_o'] = c_I I$, where $c_I = \frac{1}{2^{d_1}} \operatorname{Tr}(I M_o) = \frac{1}{2^{d_1}} \operatorname{Tr}(M_o) = \frac{1}{2^{d_1}}$. Thus, $\mathbb{E}_k(M_o') = \frac{I_{2^{d_1}}}{2^{d_1}}$, and hence, $\mathbb{E}_{k'}[M_c''] = \frac{I_{2^{d_2}}}{2^{d_2}}$.

Similarly, for the covert message $M_c \in (\mathbb{C}^2)^{\otimes d_2}$, the encrypted state is $M_c' = U_{k'} M_c U_{k'}^\dagger$, with $k' \in \{0,1\}^{2d_2}$ and we have $\mathbb{E}_{k'}[M_c'] = \frac{I_{2^{d_2}}}{2^{d_2}}$.

We compute $\mathbb{E}_l[\sigma_l X \sigma_l^\dagger]$, for a fixed matrix X of compatible dimension. The set of all permutation matrices forms a group under multiplication.

Then we have,

$$\mathbb{E}_l[M_f^{(1)}] = \frac{1}{(2^{d_1+1})!} \sum_{l \in \mathrm{Sym}(2^{d_1+1})} \sigma_l M_f^{(1)} \sigma_l^\dagger. \tag{85}$$

The representation of $\mathrm{Sym}(n)$ is defined by $\pi : \mathrm{Sym}(n) \longrightarrow \mathcal{U}(\mathbb{C}^n)$ by

$$\pi(\sigma)\, e_i = e_{\sigma(i)}, \quad \text{for} \quad i = 1, \ldots, n, \tag{86}$$

where $\{e_i\}_{i=1}^n$ is the standard orthonormal basis of $\mathbb{C}^n$ and $\mathcal{U}(\mathbb{C}^n)$ denotes the group of unitary operators on $\mathbb{C}^n$, [See [65], [66]]. It is well known that this representation is *reducible*.

Let

$$\mathcal{A} = \{A \in \mathcal{L}(\mathbb{C}^n) :\ A\, \pi(\sigma) = \pi(\sigma) A,\ \forall\, \sigma \in \mathrm{Sym}(n)\}$$

be the centralizer or the commutant of the representation π.

By the *Double Commutant Theorem* and by applying *Schur's lemma*, $\mathcal{T}_{\mathrm{Sym}(n)}(\Phi) \in \mathcal{A}$ and $\mathcal{A} = span\{I,\, J\}$, where I is the $n \times n$ identity matrix and J is the $n \times n$ matrix such that $J_{ij} = 1$ for all $i, j \in [n]$. Then, for any matrix $\Phi \in \mathcal{L}(\mathbb{C}^n)$ we have,

$$\mathcal{T}_{\mathrm{Sym(n)}}(\Phi) = \alpha(\Phi)\, I + \beta(\Phi)\, J, \tag{87}$$

for some scalars $\alpha(\Phi), \beta(\Phi) \in \mathbb{C}$ that depend linearly on Φ. We will only denote $\mathcal{T}_{\mathrm{Sym}(n)}(\Phi)$ by only $\mathcal{T}(\Phi)$ if it is understood that we are considering the representation of $\mathrm{Sym}(n)$ only.

For any matrix $\Phi \in \mathcal{L}(\mathbb{C}^n)$, the twirl $\mathcal{T}(\Phi) = \mathbb{E}_l\left[\sigma_l\, \Phi\, \sigma_l^\dagger\right]$. We compute the coefficients $\alpha(\Phi)$ and $\beta(\Phi)$ in terms of two linear invariants of Φ:

$$T(\Phi) := \mathrm{Tr}(\Phi) \quad \text{and} \quad S(\Phi) := \sum_{i=1}^{n}\sum_{j=1}^{n} \Phi_{ij}. \tag{88}$$

Taking the trace of $\mathcal{T}(\Phi)$, we obtain

$$\alpha(\Phi) + \beta(\Phi) = \frac{T(\mathcal{T}(\Phi))}{n}. \tag{89}$$

On the other hand, the sum of all entries of $\mathcal{T}(\Phi)$ is

$$S\big(\mathcal{T}(\Phi)\big) = \alpha(\Phi)\, n + \beta(\Phi)\, n^2. \tag{90}$$

The twirling map is *trace–preserving*. As the permutation conjugation simply reorders the entries, the permutation twirling *preserves the sum of all matrix elements*. Therefore,

$$S\big(\mathcal{T}(\Phi)\big) = S(\Phi) \quad \text{and} \quad T\big(\mathcal{T}(\Phi)\big) = T(\Phi). \tag{91}$$

Thus,

$$\alpha(\Phi)\, n + \beta(\Phi)\, n^2 = S(\Phi) \quad \text{and} \quad n(\alpha(\Phi) + \beta(\Phi)) = T(\Phi). \tag{92}$$

Solving both the equations 92, we get,

$$\beta(\Phi) = \frac{S(\Phi) - T(\Phi)}{n(n-1)} \quad \text{and} \quad \alpha(\Phi) = \frac{nT(\Phi) - S(\Phi)}{n(n-1)}. \tag{93}$$

Now, considering $\Phi = M_a^{(0)}$, we get

$$\alpha(M_a^{(0)}) = \frac{2^{d_1+1} - S(\Phi)}{2^{d_1+1}(2^{d_1+1}-1)}. \tag{94}$$

Since $M_a^{(0)}$ is diagonal and constant along the diagonal, its off-diagonal entries are zero so that

$$S\big(M_a^{(0)}\big) = \sum_{i=1}^{2^{d_1+1}} \sum_{j=1}^{2^{d_1+1}} (M_a^{(0)})_{ij} = \sum_{i=1}^{2^{d_1+1}} \frac{1}{2^{d_1+1}} = 1. \tag{95}$$

and hence, $\alpha(M_a^{(0)}) = \frac{1}{2^{d_1+1}}$ and $\beta\big(M_a^{(0)}\big) = 0$. Therefore,

$$\mathbb{E}_l\big[M_f^{(0)}\big] = \alpha\big(M_a^{(0)}\big)\, I + \beta\big(M_a^{(0)}\big)\, J = \frac{I}{2^{d_1+1}}. \tag{96}$$

Now, consider the quantum density matrix $\Phi = M_a^{(1)}$. Then, after taking expectation $\mathbb{E}_k[M_o']$ and $\mathbb{E}_{k'}[M_c'']$ separately, we get, $T\big(M_a^{(1)}\big) = 1 \quad \text{and} \quad S\big(M_a^{(1)}\big) = \Big(1 + \frac{2}{\eta}\Big)$.
Computing the coefficients $\alpha(\Phi)$ and $\beta(\Phi)$, we get,

$$\alpha\big(M_a^{(1)}\big) = \frac{2^{d_1+1} - 1 - \frac{2}{\eta}}{2^{d_1+1}(2^{d_1+1}-1)} \quad \text{and} \quad \beta\big(M_a^{(1)}\big) = \frac{2/\eta}{2^{d_1+1}(2^{d_1+1}-1)}. \tag{97}$$

Therefore,

$$\mathbb{E}_l\big[M_f^{(1)}\big] = \alpha\big(M_a^{(1)}\big)\, I + \beta\big(M_a^{(1)}\big)\, J = \frac{2^{d_1+1} - 1 - \frac{2}{\eta}}{2^{d_1+1}(2^{d_1+1}-1)} I \;+\; \frac{2/\eta}{2^{d_1+1}(2^{d_1+1}-1)} J. \tag{98}$$

Now, computing difference we get,

$$\mathbb{E}_l\big[M_f^{(1)}\big] - \mathbb{E}_l\big[M_f^{(0)}\big] = \frac{2}{\eta 2^{d_1+1}(2^{d_1+1}-1)}(J - I). \tag{99}$$

It is well-known that, one eigen value of the matrix $(J - I)$ is $(2^{d_1+1} - 1)$ and the eigenvalue -1 has multiplicity $(2^{d_1+1} - 1)$.

Therefore, the trace distance is

$$\begin{aligned} D\Big(\mathbb{E}_l\big[M_f^{(1)}\big], \mathbb{E}_l\big[M_f^{(0)}\big]\Big) &= \frac{1}{2}\,\|\mathbb{E}_l\big[M_f^{(1)}\big] - \mathbb{E}_l\big[M_f^{(0)}\big]\|_1 \\ &= \frac{1}{2}\Big[\frac{2}{\eta 2^{d_1+1}(2^{d_1+1}-1)}\|(J-I)\|_1\Big] \\ &= \frac{1}{2}\cdot\frac{4}{\eta\, 2^{d_1+1}(2^{d_1+1}-1)}(2^{d_1+1}-1) \\ &= \frac{1}{\eta\, 2^{d_1}}. \end{aligned} \tag{100}$$

Hence, $D\Big(\mathbb{E}_l\big[M_f^{(1)}\big], \mathbb{E}_l\big[M_f^{(0)}\big]\Big) < \mathsf{negl}(\lambda)$.

Choosing two different keys $(l, d_1, d_2, k, k', \eta)$ and $(\tilde{l}, \tilde{d_1}, \tilde{d_2}, \tilde{k}, \tilde{k'}, \tilde{\eta})$ from the same set $\mathrm{Sym}(n) \times [2^{d_1+1}] \times [2^{d_1+1}] \times \{0,1\}^{d_1} \times \{0,1\}^{d_2} \times \mathcal{J}$, with uniform distribution, it is easy to see that $D(\mathbb{E}_l[M_f^{(1)}], \mathbb{E}_l[M_f^{(1)'}]) = 0$.

□

Now, we prove the computational indistinguishability of the original and anamorphic ciphertexts.

Theorem 11. *The original and anamorphic ciphertexts $M_f^{(0)}$ and $M_f^{(1)}$ are computationally indistinguishable.*

Proof. In the real game, the adversary receives the original ciphertext

$$M_f^{(0)} = \sigma_l \begin{pmatrix} \frac{1}{2}M_o' & 0 \\ 0 & \frac{1}{2}M_o' \end{pmatrix} \sigma_l^\dagger. \tag{101}$$

and in the anamorphic game, the adversary receives the following anamorphic ciphertext

$$M_f^{(1)} = \sigma_l \begin{pmatrix} \frac{1}{2}M_o' & \frac{1}{\eta}M_c'' \\ (\frac{1}{\eta}M_c'')^\dagger & \frac{1}{2}M_o' \end{pmatrix} \sigma_l^\dagger. \tag{102}$$

We know the following inequality between adversarial advantage and the trace distance $\mathrm{Adv}_{\mathcal{D}}(\lambda) \leq D(M_f^{(0)}, M_f^{(1)})$ 1.

Now, we compute the trace distance between the real and the anamorphic ciphertexts,

$$\begin{aligned} D(M_f^{(0)}, M_f^{(1)}) &= \frac{1}{2}\Big\|M_f^{(0)} - M_f^{(1)}\Big\|_1 \\ &= \frac{1}{2}\left\|\sigma_l \begin{pmatrix} \frac{1}{2}M_o' & 0 \\ 0 & \frac{1}{2}M_o' \end{pmatrix}\sigma_l - \sigma_l \begin{pmatrix} \frac{1}{2}M_o' & \frac{1}{\eta}M_c'' \\ \frac{1}{\eta}(M_c'')^\dagger & \frac{1}{2}M_o' \end{pmatrix}\sigma_l^\dagger\right\|_1 \\ &= \frac{1}{2}\left\|\sigma_l \begin{pmatrix} 0 & -\frac{1}{\eta}M_c'' \\ -\frac{1}{\eta}(M_c'')^\dagger & 0 \end{pmatrix}\sigma_l^\dagger\right\|_1 \\ &= \frac{1}{2}\left\|\begin{pmatrix} 0 & -\frac{1}{\eta}M_c'' \\ -\frac{1}{\eta}(M_c'')^\dagger & 0 \end{pmatrix}\right\|_1 (\text{ since } \sigma_l \text{ is unitary and the trace norm is unitary invariant}). \end{aligned} \tag{103}$$

As, M_c is a Hermitian, positive semi-definite matrix with $\mathrm{Tr}(M_c) = 1$, after encrypting with the key k' the density matrix $M_c' = \mathsf{QOTP}(M_c, k')$, remains as Hermitian, positive semi-definite and preserves the norm. Hence, $\frac{1}{\eta}M_c'' = \frac{1}{\eta}(M_c'')^\dagger$.

Denote the matrix $\begin{pmatrix} 0 & -\frac{1}{\eta}M_c'' \\ -\frac{1}{\eta}(M_c'')^\dagger & 0 \end{pmatrix}$ by A.

Then

$$A^2 = \begin{pmatrix} \frac{1}{\eta^2}(M_c'')^2 & 0 \\ 0 & \frac{1}{\eta^2}(M_c'')^2 \end{pmatrix}. \tag{104}$$

The trace norm of A is

$$\|A\|_1 = \mathrm{Tr}(\sqrt{A^2}) = \frac{2}{\eta}.\,\mathrm{Tr}(M_c'') = \frac{2}{\eta}. \tag{105}$$

Thus, the trace distance is

$$D(M_f^{(0)}, M_f^{(1)}) = \frac{1}{2}\|M_f^{(0)} - M_f^{(1)}\|_1 = \frac{1}{2}\|A\|_1 = \frac{1}{2}\cdot\frac{2}{\eta} = \frac{1}{\eta} < \mathsf{negl}(\lambda). \tag{106}$$

□

Note that as we have remarked earlier 1 that the algorithm DOM can be applied to both $M_f^{(0)}$ and $M_f^{(1)}$. The dictator and the players can decryprt the original ciphertext M_o from both the ciphertexts $M_f^{(0)}$ and $M_f^{(1)}$ exactly using the same DOM algorithm. Therefore, both the ciphertexts $M_f^{(0)}$ and $M_f^{(1)}$ are indistinguishable to the dictator.

In quantum mechanics, fidelity is a metric used to quantify the similarity or closeness between quantum states. A high fidelity value indicates that the states are nearly identical. In our case, as a consequence of negligible trace distance, it is easy to show that the original and anamorphic quantum states exhibit a high fidelity. Consequently, this establishes that, in our case, an adversary or dictator is computationally unable to distinguish between the ciphertexts $M_f^{(0)}$ and $M_f^{(1)}$, making it infeasible to identify which corresponds to the original ciphertext.

Theorem 12. *The fidelity between the original and the anamorphic states is*

$$F(M_f^{(0)}, M_f^{(1)}) \geq \left(1 - \frac{1}{\eta}\right)$$

indicating that the two states are nearly indistinguishable for large η.

Proof. By the Fuchs-van de Graaf inequality, and Theorem 11, $\left(1 - F(M_f^{(1)}, M_f^{(0)})\right) \leq \frac{1}{\eta}$.
Hence,

$$F(M_f^{(1)}, M_f^{(0)}) \geq \left(1 - \frac{1}{\eta}\right).$$

□

Now we describe the communication procedure between Alice and Bob under dictatorial supervision.

Algorithm 5 Transmission Protocol under Dictatorial Supervision (TPDS)

Input: Anamorphic state $M_f^{(1)} \in \mathcal{L}((\mathbb{C}^2)^{\otimes(d_1+1)})$, dimensions d_1, d_2, keys k, k', and permutation matrix σ_l.
Output: The original message M_o for both Bob and the dictator, and the covert message M_c exclusively for Bob.
Step 1: Alice's Transmission to Bob:
Alice generates the anamorphic encrypted state $M_f^{(1)}$ using the encryption process.
Alice transmits:

$$M_f^{(1)}, \quad (l, d_1, d_2, k, k', \eta)$$

securely to Bob.
Step 2: Bob's Decryption:
Bob receives $M_f^{(1)}$ and the keys l, d_1, d_2, k, k', η.
Bob performs the following operations:

1) Run the **Decryption of Original Message (**DOM**)** algorithm with the key k to recover the original message M_o.
2) Run the **Covert Decryption of Anamorphic Message (**DCM**)** algorithm with key k' to recover the covert message M_c.

Step 3: Bob's Forwarding to the Dictator:
Bob forwards to the dictator the following information:

$$M_f^{(1)}, \quad (l, d_1, k).$$

Step 4: Dictator's Decryption:
The dictator receives $M_f^{(1)}$ and keys l, d_1, k.
The dictator runs the **Decryption of Original Message (**DOM**)** algorithm using key k to recover the original message M_o.
Step 6: Output:
Bob receives both M_o and M_c.
The dictator receives only M_o.

VI. Anamorphic Secret-Sharing

In this section, our main goal is to define quantum anamorphic secret-sharing. First, we will review basic notions of quantum secret-sharing schemes. Then we will propose a definition of a quantum anamorphic secret-sharing along with our construction.

With abuse of notation, we denote $P \subseteq [n]$ to be a set of players. Let $\mathcal{S}$ be a set of secrets. Let $\mathcal{R}$ be a finite set of random strings, $\mu : \mathcal{R} \longrightarrow \mathbb{R}$ be a probability distribution function, and $\forall j,\ 1 \leq j \leq n,\ \mathcal{S}_j$ be the domain of shares of j-th player.

In a secret-sharing scheme, we want to share a secret among n players so that

- only the authorized set of players can reconstruct the secret and
- the unauthorized set of players cannot reconstruct the secret.

Definition 16. *[20] A sequence of monotone functions $(f_n)_{n\in\mathbb{Z}^+}$, where each function $f_n \colon \{0,1\}^n \longrightarrow \{0,1\}$ is computable by a family of monotone circuits of size polynomial in n, based on the existence of one-way functions, is defined as belonging to the class* monotone P.

We refer to the survey article by [34] for detailed exposition. We can define the *access structure* by a monotone function $f \colon \{0,1\}^n \longrightarrow \{0,1\}$ with a set $P \subseteq [n]$ defined to be authorized if and only if $f(v^P) = 1$ where $v^P \in \{0,1\}^n$ the characteristic vector of P satisfying $v_i^P = 1$ when $i \in P$ [20]. We denote the t out of n threshold function by T_n^t such that $T_n^t(P) = 1$ if and only if $|P| \geq t$.

• **Key difficulty in quantum secret sharing due to no-cloning theorem:** The *no-cloning theorem* [21] prevents copying unknown quantum states, which makes quantum secret sharing difficult. This prevents fundamental strategies like sharing components with multiple players. In other words, no quantum secret-sharing techniques realize the OR function. The methodologies behind many important classical conclusions cannot be readily transferred to the quantum setting, therefore lifting them requires new thinking. We now detail our contributions and formal outcomes. A small generic compiler using hybrid encoding from classical to quantum secret sharing that we construct and analyze yields our results. However, this problem was addressed in the work of Chien [70], and also in the work of Çakan et. al. [20].

• **Heavy monotone functions:** This concept was introduced in the work of Çakan et. al. [20]. The no-cloning theorem limits quantum secret sharing systems to *no-cloning* monotone functions. These monotone functions f are defined such that $f(P) = 1$ implies $f(P) = 0$, meaning the complement of an authorized set is unauthorized. The state-of-the-art share size for all no-cloning monotone functions f is the size of the smallest monotone span program computing f, which can be very large even for “simple” no-cloning monotone functions in monotone P.

Definition 17. *(Heavy function [20]) A monotone function $f \colon \{0,1\}^n \longrightarrow \{0,1\}$ is said to be t-heavy if for any subset $P \subseteq [n]$ where $f(P) = 1$, it holds that $|P| \geq t$. For $t \geq \lfloor n/2 \rfloor + 1$, we say that f is heavy.*

Note that t-heavy monotone functions are those with a *minimum authorized set* size of at least t. Note that a t-out-of-n threshold function is a type of t-heavy function.

Proposition 13. *([20]) Let $\mathsf{mSP}(f)$ and $\mathsf{mC}(f)$ be the size of smallest monotone span program and monotone circuit for computing f, respectively. Then, for every monotone function $f \colon \{0,1\}^n \longrightarrow \{0,1\}$ there exist a heavy monotone function $f \colon \{0,1\}^{2n} \longrightarrow \{0,1\}$ such that $\mathsf{mSP}(f') \geq \frac{\mathsf{mSP(f')}}{2n}$ and $\mathsf{mC}(f') \leq \mathsf{mC}(f) + n$. Also, whenever $f \in \mathsf{mNP}$, then $f' \in \mathsf{mNP}$.*

Corollary 13.1. *([20]) There exist heavy monotone functions in* monotone P *requiring monotone span programs of size* $\exp(n^{\Omega(1)})$.

• **Sharing multiple copies bypassing the no-cloning theorem:** Not all monotone functions can be implemented by conventional quantum secret sharing protocols due to the no-cloning theorem and due to that, we need some additional assumptions to design quantum secret-sharing schemes for a wide range of monotone functions [20]. One solution to this problem is to assume that we have access to several copies of the quantum state that we want to share [20]. In the multiparty computations(MSP), this makes sense. The classical description of their quantum input is already known to each player and they can create as many copies as they want. The work of [70] considered a special case of threshold monotone functions and investiated the number of copies we would require to construct an efficient secret-sharing scheme realizing all monotone functions in monotone P [20]. Chien showed without security proof that $\max(1, n - 2t + 2)$ copies of the quantum secret are sufficient to construct a t-out-of-n quantum secret-sharing scheme [20], [70].

A. Classical secret-sharing scheme

In this section, we review some basic definitions of the theory of classical secret-sharing schemes.

Definition 18. *(Classical secret-sharing scheme [20], [34]) A classical perfect secret-sharing scheme realizing the monotone function* $f\colon \{0,1\}^n \longrightarrow \{0,1\}$ *is a pair of functions* $\mathsf{SS} = (\mathsf{Share}, (\mathsf{Rec}_P)_{P\subseteq[n]})$

where $\mathsf{Share} : \mathcal{S}\times\mathcal{R} \longrightarrow \mathcal{S}_{[n]}$ *and* $\mathsf{Rec}_P : \mathcal{S}_P \longrightarrow \mathcal{S}$ *are deterministic functions satisfying the following properties for all* $P \subseteq [n]$*:*

- ***Correctness**: If* $f(P) = 1$*, then for all* $s \in \mathcal{S}$*,*

$$\Pr_{R\leftarrow\mathcal{R}}[\mathsf{Rec}_P(\mathsf{Share}(s;R)_P) = s] = 1.$$

- ***Perfect Privacy**: If f(P) = 0, then for all secrets* $s_1, s_2 \in \mathcal{S}$ *and share vectors* $v \in \mathcal{S}_P$*, we have*

$$\Pr_{R\leftarrow\mathcal{R}}[\mathsf{Share}(s_1;R)_P = v] = \Pr_{R\leftarrow R}[\mathsf{Share}(s_2;R)_P = v].$$

Definition 19. *(Share size [20]) For a secret-sharing scheme* SS *defined over the share domains* $\{\mathcal{S}_1,\dots,\mathcal{S}_n\}$*, the share size, denoted as* size(SS)*, is given by*

$$\mathsf{size}(\mathsf{SS}) = \sum_{i=1}^{n}\lceil\log|\mathcal{S}_i|\rceil.$$

This represents the total number of bits required to encode all shares in the scheme.

Definition 20. *(Statistical privacy for classical secrets [20]) A secret-sharing scheme* SS *that realizes a monotone function* f *is said to be* ε*-statistically private if, for any subset* $P \subseteq [n]$ *where* $f(P) = 0$ *and for any two secrets* $s_1, s_2 \in \mathcal{S}$*, the following holds:*

$$\Delta(\mathsf{Share}(s_1;R_1)_P, \mathsf{Share}(s_2;R_2)_P) \le \varepsilon,$$

where $R_1 \leftarrow \mathcal{R}$ *and* $R_2 \leftarrow \mathcal{R}$ *are independent random variables.*

Definition 21. *(Post-quantum computational privacy for classical secrets [20]) A secret-sharing scheme* SS *that realizes a monotone function* f *is considered post-quantum computationally private if, for any subset* $P \subseteq [n]$ *where* $f(P) = 0$*, any two secrets* $s_1, s_2 \in \mathcal{S}$*, and any QPT (quantum polynomial-time) adversary* $\{C_\lambda\}_\lambda$*, the following holds:*

$$\left|\Pr_{R\leftarrow\mathcal{R}}\left[C_\lambda(\mathsf{Share}(s_1;1^\lambda,R)_P) = 1\right] - \Pr_{R\leftarrow\mathcal{R}}\left[C_\lambda(\mathsf{Share}(s_2;1^\lambda,R)_P) = 1\right]\right| \le \mathsf{negl}(\lambda).$$

In a (t,n)-threshold secret-sharing scheme, Ogata et al. introduced the concept of *security against cheaters* [Section 4.1, [47]]. Building upon this concept, we propose an extension to this definition, termed *security against partial cheating*, which serves as a property to defend against potential attacks.

For each participant P_i the share is given by $s_i^{(a)} = \big(s_{i_1}^{(a)}, s_{i_2}^{(a)}, \dots, s_{i_m}^{(a)}\big)$, for some integer m and is written into two parts, $s_i^{(a)} = \big(s_i^{(o)}, s_i^{(c)}\big)$, where $s_i^{(o)}$ is the *original share part*, and $s_i^{(c)}$ is the *covert share part*. Let $X_{\mathcal{S}^{(o)}}$ and $X_{\mathcal{S}^{(c)}}$ be the random variable defined over the original and the covert part of the secret spaces in $\mathcal{S}$ and $V_i^{(a)}$ be the random variable induced by $s_i^{(a)}$. Let

$$supp(V_i^{(a)}) = \{\, s_i^{(a)} \mid \Pr\Big(V_i^{(a)} = s_i^{(a)}\Big) > 0 \,\}$$

denote the support of the share vector $s_i^{(a)}$ for participant P_i. For a given t-tuple of shares

$$w^{(a)} = \Big((s_{i_1}^{(o)}, s_{i_1}^{(c)}),\ (s_{i_2}^{(o)}, s_{i_2}^{(c)}),\ \dots,\ (s_{i_t}^{(o)}, s_{i_t}^{(c)})\Big)$$

in the product space

$$supp(V_{i_1}^{(a)}) \times supp(V_{i_2}^{(a)}) \times \cdots \times supp(V_{i_t}^{(a)}),$$

we define the *partial reconstruction function* $\mathsf{Sec}^{(o)}$ by

$$\mathsf{Sec}^{(o)}(w^{(a)}) = \begin{cases} s^{(o)}, & \text{if } \exists s^{(o)} \text{ s.t. } \Pr\Big(X_{\mathcal{S}^{(o)}} = s^{(o)} \mid V_{i_1}^{(a)}, \dots, V_{i_t}^{(a)} = w^{(a)}\Big) = 1,\\ \perp, & \text{otherwise.}\end{cases}$$

and

$$\mathsf{Sec}^{(c)}(w^{(a)}) = \begin{cases} s^{(c)}, & \text{if } \exists s^{(c)} \text{ s.t. } \Pr\Big(X_{S^{(c)}} = s^{(c)} \mid V_{i_1}^{(a)}, \ldots, V_{i_t}^{(a)} = w^{(a)}\Big) = 1, \\ \perp, & \text{otherwise.} \end{cases}$$

Thus, when the t players provide their correct shares

$$b = \Big((s_{i_1}^{(o)}, s_{i_1}^{(c)}),\, (s_{i_2}^{(o)}, s_{i_2}^{(c)}),\, \ldots,\, (s_{i_t}^{(o)}, s_{i_t}^{(c)})\Big),$$

we have

$$\mathsf{Sec}^{(p)}(b) = (\mathsf{Sec}^{(o)}(b), \mathsf{Sec}^{(c)}(b)) = \big(s^{(o)}, s^{(c)}\big) = s.$$

Let b denote the honest share tuple:

$$b = \Big((s_{i_1}^{(o)}, s_{i_1}^{(c)}),\, (s_{i_2}^{(o)}, s_{i_2}^{(c)}),\, \ldots,\, (s_{i_t}^{(o)}, s_{i_t}^{(c)})\Big).$$

Now, consider a forged share tuple

$$b' = \Big((s_{i_1}^{(o)}, s_{i_1}^{(c)'}),\, (s_{i_2}^{(o)}, s_{i_2}^{(c)'}),\, \ldots,\, (s_{i_t}^{(o)}, s_{i_t}^{(c)'})\Big)$$

with the property that for every $j \in \{1, 2, \ldots, t\}$ the original part is unchanged:

$$s_{i_j}^{(o)} \text{ in } b' = s_{i_j}^{(o)} \text{ in } b,$$

while there exists at least one index j such that

$$s_{i_j}^{(c)'} \neq s_{i_j}^{(c)}.$$

We say that the dictator $\mathcal{D}$ is *partially cheated* by the forged tuple b' if

$$\mathsf{Sec}^{(p)}(b') \in \mathcal{S} \quad \text{and} \quad \mathsf{Sec}^{(p)}(b') \neq \mathsf{Sec}^{(p)}(b).$$

That is, although $\mathcal{D}$ reconstructs the correct original component $s^{(o)}$, the covert component $s^{(c)}$ is altered due to the substitution of forged shares.

Definition 22. *([47]) For a coalition of t players $P_{i_1}, \ldots, P_{i_t}$ with covert shares $b^{(c)} = (s_{i_1}^{(c)}, \ldots, s_{i_t}^{(c)})$, define the partial cheating probability as:*

$$\mathsf{Cheat}^{(p)}\left(V_{i_1}^{(a)}, \ldots, V_{i_t}^{(a)}\right) := \max_{b} \max_{b'} \Pr\left(\mathcal{D} \textit{ is cheated by } b' \mid\; P_{i_1}, \ldots, P_{i_t} \textit{ have } b\right).$$

B. Quantum erasure-correcting codes

We have used the following description of quantum erasure correcting code, described by Çakan et al. from the paper [20].

Definition 23. *(Quantum Erasure Correcting Code(QECC) [20]) A pair of trace-preserving quantum operations, denoted as $\mathsf{QC} = (\mathsf{QC.Enc}, \mathsf{QC.Dec})$, is referred to as a quantum erasure correcting code (QECC) over the input space $\mathcal{H}_{inp}$ and the output space $\mathcal{H}_{out} = \bigotimes_{i\in[n]} \mathcal{H}_i$ for a subset $P \subseteq [n]$, if for any quantum operation Υ acting on $\mathcal{H}_{out}$ that preserves the identity on $\mathcal{H}_i$ for all $i \in P$, the following condition holds for any quantum state ρ in $\mathcal{H}_{inp}$:*

$$(\mathsf{QC.Dec} \circ \Upsilon \circ \mathsf{QC.Enc})(\rho) = (\rho \otimes \sigma)$$

for some fixed quantum state σ.

If $(\mathsf{QC.Enc}, \mathsf{QC.Dec}_P)$ serves as a Quantum Error-Correcting Code (QECC) for all subsets $P \subseteq [n]$ where a monotone function $f : \{0,1\}^n \longrightarrow \{0,1\}$ satisfies $f(P) = 1$, then the collection of operations $(\mathsf{QC.Enc}, (\mathsf{QC.Dec}_P)_{P\subseteq[n]})$ is said to realize f as a QECC. The code reconstruction function is defined as follows:

$$\mathsf{QC.Rec}_P(\tau) = \mathsf{QC.Dec}(\tau \otimes (|0\rangle\langle 0|)^{\otimes \overline{P}}).$$

A quantum error-correcting code that encodes k q-ary qudits into n q-ary qudits and can recover from up to $(d-1)$ erasures is referred to as a $[[n, k, d]]_q$ code.

C. Quantum secret-sharing scheme

Secret sharing involves dividing a secret into multiple parts, which are then distributed to different players. Only when these parts are combined, the original secret can be reconstructed. In a quantum anamorphic secret-sharing scheme, not only would the secret be protected by quantum-resistant cryptographic methods, but an additional covert secret is encoded into the shares themselves. This ensures that even if a quantum adversary were to intercept or analyze some of these shares, they would be unable to detect the existence of the hidden message without the appropriate classical or quantum key.

For a rigorous description about quantum secret-sharing model we refer [20], [45] to the reader.

Definition 24. *(No-cloning function [20]) A monotone function $f\colon \{0,1\}^n \longrightarrow \{0,1\}$ is said to satisfy the no-cloning property and called no-cloning function if, for every subset $P \subseteq [n]$, it holds that $f(\overline{P}) = 0$ while $f(P) = 1$.*

Let the Hilbert space $\mathcal{S}$ be the domain of secret, and the Hilbert spaces $\mathcal{H}_1, \ldots, \mathcal{H}_n$ be the domain of shares of n players. Let $f\colon \{0,1\}^n \longrightarrow \{0,1\}$ be a no-cloning monotone function.

Definition 25. *(Quantum secret-sharing scheme [20]) A quantum secret-sharing (QSS) scheme with perfect privacy that realizes a monotone function f is defined as a set of trace-preserving quantum operations:*

$$\mathsf{QSS} = (\mathsf{Share}, (\mathsf{Rec}_P)_{P\subseteq[n]})$$

that satisfy the following conditions for all subsets $P \subseteq [n]$:
- ***Correctness:** If $f(P) = 1$, then the pair $(\mathsf{Share}, \mathsf{Rec}_P)$ forms a quantum error-correcting code (QECC) for P, ensuring that the secret can be reconstructed.*
- ***Perfect Privacy**: If $f(P) = 0$, then for any two quantum states $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{S}$, the marginal distributions over the shares outside P remain identical, i.e.,*

$$\mathrm{Tr}_{\overline{P}}(\mathsf{Share}(|\psi_1\rangle\langle\psi_1|)) = \mathrm{Tr}_{\overline{P}}(\mathsf{Share}(|\psi_2\rangle\langle\psi_2|)).$$

This property ensures that unauthorized subsets gain no information about the quantum secret.

A quantum secret-sharing scheme (QSS) is considered *efficient* if both the sharing algorithm ($\mathsf{QSS.Share}$) and the reconstruction algorithm ($\mathsf{QSS.Rec}$) can be implemented using polynomial-size circuits [20]. Additionally, in efficient schemes, the size of each share is also polynomially bounded [20].

Definition 26. *(Statistical privacy for quantum secrets [71] [20]) A quantum secret-sharing scheme (QSS) that realizes a monotone function f is said to be ε-statistically private if, for every subset $P \subseteq [n]$ where $f(P) = 0$, and for any two secrets $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{S}$, the following condition holds:*

$$D(\mathrm{Tr}_{\overline{P}}(\mathsf{Share}(|\psi_1\rangle\langle\psi_1|)), \mathrm{Tr}_{\overline{P}}(\mathsf{Share}(|\psi_2\rangle\langle\psi_2|))) \leq \varepsilon.$$

Note that the perfect privacy means here 0-statistical privacy.

Definition 27. *(Computational privacy for quantum secrets [20]) A quantum secret-sharing scheme (QSS) that realizes f is considered computationally private if, for any subset $P \subseteq [n]$ where $f(P) = 0$, any two secrets $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{S}$, and any QPT (quantum polynomial-time) adversary $\{C_\lambda\}_\lambda$, the following holds:*

$$\left|\Pr\left[C_\lambda(\mathrm{Tr}_{\overline{P}}(\mathsf{Share}(|\psi_1\rangle\langle\psi_1|; 1^\lambda))) = 1\right] - \Pr\left[C_\lambda(\mathrm{Tr}_{\overline{P}}(\mathsf{Share}(|\psi_2\rangle\langle\psi_2|; 1^\lambda))) = 1\right]\right| \leq \mathsf{negl}(\lambda).$$

Definition 28. *(Information ratio of a quantum secret-sharing scheme [34] [20]). If a secret is composed of t qubits then the information ratio of a quantum secret-sharing scheme is defined by*

$$\frac{\max_{i\in[n]} |\mathcal{S}_i|}{t}$$

1) Quantum Anamorphic Secret-Sharing Schemes

In this section, we introduce the notion of an *anamorphic secret-sharing*. In our proposed mathematical model, there is a *dictator* $\mathcal{D}$, who is a passive adversary here, a *dealer* D who distributes shares to a set of n players according to predefined access structures, in the presence of the *dictator* ensuring the correctness and privacy properties of the anamorphic secret-sharing scheme. The dealer aims to send two messages: an original message and a covert message, to the set of players. After the encryption of these two messages, combining these two ciphertexts we construct the anamorphic ciphertext which is computationally indistinguishable from the original ciphertext to the dictator. The dealer now sends the anamorphic ciphertext to the set of players along with the keys to decrypt those messages.

The dealer sends the anamorphic ciphertext and the anamorphic key to the set of n players. The authorized set of players reconstructs the original key and the covert key and then shares the original key with the dictator along with the anamorphic ciphertext. The dictator extracts the original message from the anamorphic ciphertext and then verifies the original message, that he wanted to send. The dictator cannot distinguish between original and anamorphic ciphertexts, because of the indistinguishability property and using the same decryption algorithm DOM that can be applied to both original and anamorphic ciphertext to extract the same original message from either of the ciphertexts.

Let $\mathcal{S}$ be a secret space, and let $s, \hat{s} \in \mathcal{S}$ be the original and covert secrets, respectively. Let $\mathcal{S}_1, \cdots, \mathcal{S}_n$ be the domain of shares of the players. Let $\mathsf{k}^{(o)}, \mathsf{k}^{(a)} \in \mathsf{K}$ be the normal or the original key and the anamorphic key, respectively. The anamorphic key $\mathsf{k}^{(a)} = (\mathsf{k}^{(o)}, \mathsf{k}^{(c)})$ consists of both the original and the covert keys. Let $\mathsf{ASS.Share}, \mathsf{ASS.Rec}^{\mathsf{Original}}_{P\subseteq[n]}, \mathsf{ASS.Rec}^{\mathsf{Covert}}_{P\subseteq[n]}$ denote the share function for the combined anamorphic message, the normal reconstruction function to reconstruct the original message, and the reconstruction function to recover the covert message, respectively.

We define two encryption schemes:

- **Original message encryption scheme:**

$$\begin{aligned}\mathsf{Enc}^{(o)} :& \mathcal{S} \times \mathsf{K}^{(o)} \to \mathcal{C}^{(o)} \\ & (s, \mathsf{k}^{(o)}) \longmapsto c^{(o)}\end{aligned}$$

  with corresponding decryption function $\mathsf{Dec}^{(o)}$.
- **Covert message encryption scheme:**

$$\begin{aligned}\mathsf{Enc}^{(c)} :& \mathcal{S} \times \mathsf{K}^{(c)} \longrightarrow \mathcal{C}^{(c)} \\ & (\hat{s}, \mathsf{k}^{(c)}) \longmapsto c^{(c)}\end{aligned}$$

  with corresponding decryption function $\mathsf{Dec}^{(c)}$.

We introduce an efficiently computable embedding function to construct the anamorphic message:

$$\Theta : \mathcal{C}^{(o)} \times \mathcal{C}^{(c)} \longrightarrow \mathcal{C}^{(a)}$$

which produces an anamorphic ciphertext $c^{(a)} = \Theta(c^{(o)}, c^{(c)})$. Additionally, we assume the existence of an efficient extraction algorithm:

$$\mathsf{EOC} : \mathcal{C}^{(a)} \longrightarrow \mathcal{C}^{(o)}$$

such that for all $c^{(o)}$ and $c^{(c)}$, we have:

$$\mathsf{EOC}(\Theta(c^{(o)}, c^{(c)})) = c^{(o)}.$$

Let the anamorphic key be defined as:

$$\mathsf{k}^{(a)} = (\mathsf{k}^{(o)}, \mathsf{k}^{(c)}) \in \mathsf{K}^{(o)} \times \mathsf{K}^{(c)},$$

and let $\mathcal{R}$ be a randomness space with distribution μ. Define $\mathcal{K} = \mathsf{K}^{(a)} \times \mathcal{R}$, where $\mathsf{K}^{(o)} \times \mathsf{K}^{(c)} = \mathsf{K}^{(a)}$.

For $b \in \{0, 1\}$, we define $c^{(b)}$, where $c^{(0)} = c^{(o)}$ defines the *original ciphertext* and $c^{(1)} = c^{(a)}$ defines the *anamorphic ciphertext*.

Definition 29. *(Anamorphic Secret Sharing(ASS)) An anamorphic secret-sharing scheme(ASS) with perfect privacy realizing the monotone function $f \colon \{0,1\}^n \longrightarrow \{0,1\}$ is formally defined as a tuple $\Sigma_{\mathsf{ASS}} = (\mathsf{ASS.Share}, \mathsf{ASS.Rec}^{\mathsf{AM}}_{\mathsf{P}\subseteq[\mathsf{n}]})$, where $\mathsf{ASS.Rec}^{\mathsf{AM}}_{\mathsf{P}\subseteq[\mathsf{n}]} = (\mathsf{ASS.Rec}^{\mathsf{Original}}_{P\subseteq[n]}, \mathsf{ASS.Rec}^{\mathsf{Covert}}_{P\subseteq[n]})$. Each of the deterministic functions is defined as follows:*

- ***Anamorphic Share Distribution:***

$$\begin{aligned}\mathsf{ASS.Share} :& \mathcal{S} \times \mathcal{S} \times \mathcal{K} \longrightarrow \mathcal{C}^{(a)} \times \mathcal{S}_{[n]}. \\ & (s, \hat{s}, \kappa^{(a)}) \longmapsto \left(c^{(a)}, s_1^{(a)}, \cdots, s_n^{(a)}\right)\end{aligned}$$

where $\mathcal{K} := \mathsf{K} \times \mathcal{R}$, with $\kappa^{(a)} = (\mathsf{k}^{(a)}, r)$ with r randomly chosen from a distribution $\mu : \mathcal{R} \longrightarrow \mathbb{R}$, and $\kappa^{(a)} = (\kappa^{(o)}, \kappa^{(c)})$ consists of both original and covert parts. Using a secret-sharing scheme with access structure f, distribute the original key $\mathsf{k}^{(o)}$ into shares $\{s_i^{(o)}\}_{i=1}^n$ and the covert key $\mathsf{k}^{(c)}$ into shares $\{s_i^{(c)}\}_{i=1}^n$. Each player i receives the key share $s_i^{(a)} = (s_i^{(o)}, s_i^{(c)})$.

- ***Reconstruction of the original share:*** *For any authorized subset $P \subseteq [n]$ with $f(P) = 1$, there exist deterministic reconstruction functions, $\mathsf{Rec}_P^{(\mathsf{key}_o)}$, which is the original key reconstruction function, and $\mathsf{ASS.Rec}_P$ that reconstruct the original secret s, is defined by the following commutative diagram:*

$$\mathsf{Rec}_P^{(\mathsf{key}_o)} : \mathcal{S}_P \longrightarrow \mathsf{K}^{(o)}$$

$$\begin{array}{ccc} \mathcal{C}^{(a)} \times \mathcal{S}_P & \xrightarrow{\mathsf{Rec}_P^{(\mathsf{key}_o)}} & \mathcal{C}^{(a)} \times \mathsf{K}^{(o)} \\ & \searrow^{\mathsf{Dec}^{(\mathsf{o})} \circ \mathsf{Rec}_{\mathsf{P}}^{(\mathsf{key_o})}} & \downarrow \mathsf{Dec}^{(o)} \\ & & \mathcal{S} \end{array}$$

where $\mathsf{Dec}^{(\mathsf{o})}$ *refers to the decryption of the original message algorithm,* $\mathsf{Rec}_P^{(\mathsf{key}_o)}(c^{(a)}, s_P^{(o)}) = (c^{(a)}, \mathsf{k}^{(o)})$*,* $\mathsf{Dec}^{(\mathsf{o})}(c^{(a)}, \mathsf{k}^{(o)}) = s$ *and we define* $\mathsf{Rec}_{\mathsf{P}\subseteq[\mathsf{n}]}^{\mathsf{Original}} := \mathsf{Dec}^{(\mathsf{o})} \circ \mathsf{Rec}_{\mathsf{P}\subseteq[\mathsf{n}]}^{(\mathsf{key_o})}$.

• ***Reconstruction of the covert share:*** *For any authorized subset* $P \subseteq [n]$ *with* $f(P) = 1$*, there exist deterministic covert key reconstruction function* $\mathsf{Rec}_P^{(\mathsf{key}_c)}$ *and consequently,* $\mathsf{ASS.Rec}_P^{\mathsf{Covert}}$ *that reconstructs the covert secret* $\hat{s}$*, is defined by the following commutative diagram:*

$$\mathsf{Rec}_P^{(\mathsf{key}_c)} : \mathcal{S}_P \longrightarrow \mathsf{K}^{(c)}$$

$$\begin{array}{ccc} \mathcal{C}^{(a)} \times \mathcal{S}_P & \xrightarrow{\mathsf{ECC} \circ \mathsf{Rec}_P^{(\mathsf{key}_c)}} & \mathcal{C}^{(c)} \times \mathsf{K}^{(c)} \\ & \searrow^{\mathsf{Dec}^{(c)} \circ \mathsf{ECC} \circ \mathsf{Rec}_P^{(\mathsf{key}_c)}} & \downarrow \mathsf{Dec}^{(c)} \\ & & \mathcal{S} \end{array}$$

where $\mathsf{Dec}^{(\mathsf{c})}$ *refers to the decryption of the covert message algorithm,* $\mathsf{ECC} \circ \mathsf{Rec}_P^{(\mathsf{key}_c)}(c^{(a)}, s_P^{(c)}) = (c^{(a)}, \mathsf{k}^{(c)})$*. Let*

$$\mathsf{ECC} \colon \mathcal{C}^{(a)} \longrightarrow \mathcal{C}^{(o)}$$

be the deterministic covert ciphertext extraction algorithm and $\mathsf{ECC}(c^{(a)}) = c^{(c)})$*. Then,* $\mathsf{Dec}^{(\mathsf{c})}(c^{(c)}, \mathsf{k}^{(c)}) = \hat{s}$*, and we define* $\mathsf{Rec}_P^{\mathsf{Covert}} := \mathsf{Dec}^{(c)} \circ \mathsf{ECC} \circ \mathsf{Rec}_P^{(\mathsf{key}_c)}$.

An anamorphic secret-sharing scheme Σ_{ASS} *must satisfy the following properties:*

• ***Correctness:***

- ***Correctness for original secret:*** *If* $f(P) = 1$*, then for all* $s \in \mathcal{S}$*,*

$$\Pr_{R \leftarrow \mathcal{R}}\left[\mathsf{Rec}_P^{\mathsf{Original}}(\mathsf{Share}(c^{(a)}, \kappa^{(o)})_P = s\right] = 1.$$

- ***Correctness for anamorphic secret:*** *If* $f(P) = 1$*, then for all* $s, \hat{s} \in \mathcal{S}$*,*

$$\Pr_{R \leftarrow \mathcal{R}}\left[\mathsf{Rec}_P^{\mathsf{Covert}}(\mathsf{Share}(c^{(a)}, \kappa^{(c)})_P = \hat{s}\right] = 1.$$

• ***Perfect Privacy:***

- ***Privacy for the anamorphic secret:*** *If* $f(P) = 0$*, the shares reveal no information about the secrets, the anamorphic keys as well as anamorphic ciphertexts* (s, s')*. For all* $\mathsf{k}_1^{(a)}, \mathsf{k}_2^{(a)} \in \mathsf{K}$*,*

$$\Pr_{R \leftarrow \mathcal{R}}\left[(\mathsf{Share}(\kappa_1^{(a)})_P = v\right] = \Pr_{R \leftarrow \mathcal{R}}\left[(\mathsf{Share}(\kappa_2^{(a)})_P = v\right]$$

• ***Condition for covert reconstruction:*** *If* $f(P) = 1$*, then the probability of reconstructing the covert secret* $\hat{s}$ *using only original key shares* $\kappa^{(o)}$*, given that* s *has been successfully reconstructed using the original key shares* $\kappa^{(o)}$*, is zero:*

$$\Pr_{R \leftarrow \mathcal{R}}\left[\mathsf{ASS.Rec}_P^{\mathsf{Covert}}(\mathsf{ASS.Share}(c^{(a)}, \kappa^{(o)})_P) \neq \perp\right] = 0.$$

• ***Indistinguishability of original and anamorphic ciphertexts:*** *We now describe a security game in which an adversary (or dictator)* $\mathcal{D}$ *is given access to shares produced from either an original encryption or anamorphic encryption. Using the shared extraction algorithm (*EOC*), the players* extract the original key shares(possibly based on ordering) and the original ciphertext $c^{(o)}$ from the anamorphic ciphertext $c^{(a)}$*, defined as*

$$\mathsf{EOC} : \mathcal{C}^{(a)} \longrightarrow \mathcal{C}^{(o)}$$

which, on any anamorphic ciphertext $c^{(a)}$, outputs the original ciphertext $c^{(o)}$ embedded within $c^{(a)}$ and

$$\mathsf{EOK} : \{s_i^{(a)}\}_{i=1}^n \longrightarrow \{s_i^{(o)}\}_{i=1}^n$$

is a deterministic extraction algorithm that extracts original key shares from anamorphic key shares possibly based on ordering.

Note that the challenger does not provide adversary access to extraction oracles EOC *and* EOK.
Here we define the ***Real game*** *and the* ***Anamorphic game*** *as follows:*

- ***Challenge Oracle*** $\mathcal{O}$***:***
  1) *The challenger selects a random bit* $b \in \{0,1\}$.
  2) *If* $b = 0$ *(**Real Game**($\mathsf{RealG_a}(\lambda, \mathcal{D})$)):*
     a) $\mathsf{Gen_o}(1^\lambda)$*: Generate the original key* $\mathsf{k}^{(o)}$.
     b) *Compute* $c^{(o)} \leftarrow \mathsf{Enc}^{(o)}(s, \mathsf{k}^{(o)})$.
     c) *Set the challenge ciphertext* $c^* := c^{(o)}$ *and generate shares* $\left\{\, (c^{(o)}, s_i^{(o)})\,\right\}_{i=1}^n$.
  3) *If* $b = 1$ *(**Anamorphic Game**($\mathsf{AnamorphicG}_a(\lambda, \mathcal{D})$)):*
     a) $\mathsf{Gen_a}(1^\lambda)$*: Generate the anamorphic key* $\mathsf{k}^{(a)} = (\mathsf{k}^{(o)}, \mathsf{k}^{(c)})$.
     b) *Compute*
     $$c^{(a)} \longleftarrow \Theta\Big(c^{(o)}, c^{(c)}\Big).$$
     c) *Set* $c^* := c^{(a)}$ *and generate shares* $\left\{\, (c^{(a)}, s_i^{(o)})\,\right\}_{i=1}^n$.

  The adversary $\mathcal{D}$ *is given access to the challenge shares and outputs a guess* $b' \in \{0,1\}$.

Remark 2. *Here we want to emphasize that here the original ciphertext is extracted from the anamorphic ciphertext and original key shares are extracted from the anamorphic key shares, then in both shares the original key shares are the same and the challenge is to distinguish the original and anamorphic ciphertexts for the adversary. Our main goal is to hide the covert ciphertext so that the adversary cannot suspect that there is a covert message within.*

We define the advantage of $\mathcal{D}$ *in distinguishing the* Real Game *and the* Anamorphic Game *as*

$$\begin{aligned}\mathsf{Adv}_{\mathcal{D}}^{\mathsf{AME}}(\lambda) &= \Big|\Pr\big[\mathsf{RealG}_a(\lambda, \mathcal{D})\big] - \Pr\big[\mathsf{AnamorphicG_a}(\lambda, \mathcal{D})\big]\Big| \qquad (107)\\ &= \Big|\Pr\big[(\mathcal{D} \textit{ outputs } 1) \wedge (b=1)\big] - \Pr\big[(\mathcal{D} \textit{ outputs } 1) \wedge (b=0)\big]\Big|. \qquad (108)\end{aligned}$$

The scheme satisfies the indistinguishability of original and anamorphic ciphertexts *property if for all PPT adversaries* $\mathcal{D}$

$$\mathsf{Adv}_{\mathcal{D}}^{\mathsf{AME}}(\lambda) < \mathsf{negl}(\lambda).$$

In other words, an adversary (or dictator) is unable to distinguish (with a non-negligible advantage) whether the provided shares originated from an original encryption or from anamorphic encryption.

2. *To reconstruct the original message, the reconstruction procedure applied either to the original ciphertext or to the anamorphic ciphertext will produce the same original message*

$$\mathsf{Rec}_{P\subseteq[n]}^{\mathsf{Original}}(\mathsf{Share}(c^{(a)}, \kappa^{(o)}) = \mathsf{Rec}_{P\subseteq[n]}^{\mathsf{Original}}(\mathsf{Share}(c^{(o)}, \kappa^{(o)}) = s,$$

so that the dictator cannot distinguish between $c^{(o)}$ *and* $c^{(a)}$*, which one is the original ciphertext.*

Remark 3. *Note that the definition of the anamorphic secret-sharing we described here is mainly based on classical key secret-sharing* SS *Definition 18. We will interchangeably use classical secret-sharing* SS *while defining the secret-sharing algorithm and whenever we want to emphasize the classical key distribution separately.*

VII. THE COMPILER

The following compiler model has been discussed by Çakan et al. in the paper [20]. This compiler can perfectly encrypt a quantum state using classical keys. Using similar ideas with classical secret-sharing scheme of Krawczyk [72] and using some techniques from [73], [74], Çakan et al. constructed a general compiler combining classical secret-sharing scheme and quantum erasure-correcting code [Theorem 9., Page 20, [20]]. In our paper, we have generalized the construction for anamorphic quantum ciphertext using multiple keys and we have also proved the correctness and perfect privacy properties accordingly with some additional techniques.

Let $f\colon \{0,1\}^n \longrightarrow \{0,1\}$ be a monotone function and SS be the classical secret-sharing realizing f, and QECC $\mathsf{QC} = (\mathsf{QC.Enc}, \mathsf{QC.Rec})$ with n components, and for all $x \in \{0,1\}^n$ realizing some monotone function $f'(x) \geq f(x)$ which we have access to. The quantum erasure correcting code operations QC corrects erasures in the complement of all the sets $P \subseteq [n]$ such that $f'(P) = 1$ [20]. Together with a classical secret-sharing scheme SS the compiler implements a no-cloning monotone function f with a quantum error correcting code QC that achieves a suitable no-cloning monotone function $f' \geq f$, to establish a quantum secret sharing scheme QSS that realizes f [20]. To construct quantum anamorphic secret-sharing Σ_{QASS}, we want to establish $\mathsf{QASS.Share}$ algorithm to share the quantum states M_o and M_c and using The reconstruction procedure $\mathsf{QASS.Rec}^{\mathsf{AM}}_{\mathsf{P}\subseteq[\mathsf{n}]}$ the set of players $P \subseteq [n]$ reconstructs both the state M_o and M_c utilizing the decoding process for QC and the algorithm DOM and DCM.

We now describe the quantum anamorphic secret-sharing algorithm:

Algorithm 6 Quantum Anamorphic Secret Sharing (QASS)

Input: Anamorphic quantum state $M_f^{(1)}$ and players $P_1, \ldots, P_n$.
Output: Shares $(s_i^{(a)}, \mathcal{E}_i)$ for each player P_i.
Step 1: Dealer Encrypts the Quantum State:
  Dealer runs the Quantum Anamorphic Encryption algorithm QAE to create the anamorphic quantum state: $M_f^{(1)}$.
Step 2: Share Generation:
  Share the anamorphic key: Share the anamorphic key $\mathsf{k}^{(a)} \in \mathsf{K}$ using $\mathsf{SS.Share}$ which yields the classical shares $(s_1^{(a)}, \ldots, s_n^{(a)})$, that is,
$$(s_1^{(a)}, \ldots, s_n^{(a)}) = \mathsf{SS.Share}(k_1, k_2, k_3, k_4, k_5, k_6).$$
Step 3: Encode the anamorphic quantum state:
  Encode the anamorphic quantum state $M_f^{(1)}$ using $\mathsf{QC.Enc}$, which yields entangled quantum systems $(\mathcal{E}_1, \ldots, \mathcal{E}_n)$.
Step 4: Distribution of Shares:
  Set $(s_i^{(a)}, \mathcal{E}_i)$ to be the final share of the player P_i.

For convenience of writing we have written the previous anamorphic key $\mathsf{k}^{(a)} = (k, k', d_1, d_2, l, \eta)$ as $(k_1, k_4, k_2, k_5, k_3, k_6)$ in the respective order, where $\mathsf{k}^{(\mathsf{o})} = (k_1, k_2, k_3)$ is the original key and $\mathsf{k}^{(\mathsf{c})} = (k_4, k_5, k_6)$ is the covert key.

Let $\mathcal{J} \subset \mathbb{Z}^+$ be a finite set containing η. Let $f, f'\colon \{0,1\}^n \longrightarrow \{0,1\}$ be no-cloning monotone functions with the property that $f' \geq f$. We define $\xi_{M_f^{(1)}} = \mathsf{QC.Enc}(M_f^{(1)})$ and for each $i = 1, \ldots, 6$, define $\tau_{(k_i, r_i)} = |\mathsf{SS.Share}(k_i, r_i)\rangle\langle\mathsf{SS.Share}(k_i, r_i)|$, $\tau_{k_i', r} = |\mathsf{SS.Share}(k_i', r')\rangle\langle\mathsf{SS.Share}(k_i', r')|$ as the sharing of the keys k_i, k_i' with the random inputs r_is respectively.

The scheme QASS can be defined as follows:

$$\mathsf{QASS.Share}(M_f^{(1)}) = \sum_{k_1 \in \{0,1\}^{2d_1}} \sum_{k_4 \in \{0,1\}^{2d_2}} \sum_{k_2 \in \{1,\ldots,2^{d_1+1}\}} \sum_{k_5 \in \{1,\ldots,2^{d_1+1}\}} \sum_{r_1,r_2,r_3,r_4,r_5,r_6 \in \mathcal{R}} \sum_{k_3 \in \mathrm{Sym}\,(2^{d_1+1})} \sum_{k_6 \in \mathcal{J}} \frac{1}{2^{4d_1+2d_2+2}} \frac{1}{|\mathcal{R}|^6} \frac{1}{|\ \mathcal{J}\ |} \frac{1}{2^{d_1+1}!} \left[\bigotimes_{i=1}^{6} \tau_{(k_i, r_i)} \otimes \xi_{M_f^{(1)}} \right]. \tag{109}$$

and

$$\mathsf{QASS.Rec}^{\mathsf{Original}}_{P\subseteq[n]}(\sigma) = \mathsf{DOM}(\mathsf{QC.Rec}_{P\subseteq[n]}(\mathrm{Tr}_{\mathsf{key}_a}(\sigma))), \mathsf{SS.Rec}_{P\subseteq[n]}(\mathrm{Tr}_{\mathsf{state}}(\sigma)),$$

where key_a corresponds to anamorphic key and

$$\mathsf{QASS.Rec}^{\mathsf{Covert}}_{P\subseteq[n]}(\sigma) = \mathsf{DCM}(\mathsf{QC.Rec}_{P\subseteq[n]}(\mathrm{Tr}_{\mathsf{key}_a}(\sigma))), \mathsf{SS.Rec}_{P\subseteq[n]}(\mathrm{Tr}_{\mathsf{state}}(\sigma)),$$

where $\mathrm{Tr}_{\mathsf{key}_a}$ and $\mathrm{Tr}_{\mathsf{state}}$ represent the process of tracing out the subsystem associated with the shares of the key and the shares of the quantum secret, respectively. In this framework, the classical key shares are represented as qubits in basis states. However, they may also be preserved as classical shares without altering the scheme.

We describe the quantum anamorphic secret reconstruction algorithm as follows:

Algorithm 7 Quantum Anamorphic Secret Reconstruction (QASS.Rec)

Input: Shares $(s_i^{(a)}, \mathcal{E}_i)$ of each player P_i from a set of authorized players $P \subseteq [n]$.
Output: Reconstructed original message M_o and covert message M_c.
Step 1: Reconstruct the Classical Shares:
Compute the classical shared components using classical secret-sharing(SS) reconstruction:

$$\mathsf{SS.Rec}_{P\subseteq[n]}\Big((s_i^{(a)})_{i\in P}\Big) = (k_1, k_2, k_3, k_4, k_5, k_6).$$

Step 2: Reconstruct the Anamorphic State:
Compute the anamorphic quantum state using quantum reconstruction:

$$\mathsf{QC.Rec}_P\left((\mathcal{E}_i)_{i\in P}\right) = M_f^{(1)}.$$

Apply the reconstruction algorithm $\mathsf{QASS.Rec}^{\mathsf{Original}}_{\mathsf{P\subseteq[n]}}$ to reconstruct the original message.
Apply the reconstruction algorithm $\mathsf{QASS.Rec}^{\mathsf{Covert}}_{\mathsf{P\subseteq[n]}}$ to reconstruct the covert message.
Step 7: Output:
Output the reconstructed original message M_o and the covert message M_c.

Theorem 14. *Let $f, f' : \{0,1\}^n \longrightarrow \{0,1\}$ be no-cloning monotone functions satisfying $f' \geq f$. Let $\mathsf{QC} = (\mathsf{QC.Enc}, (\mathsf{QASS.Rec}^{\mathsf{AM}}_{P\subseteq[n]}))$ denote a quantum error-correcting code (QECC) that implements f', and let $\mathsf{SS} = (\mathsf{SS.Share}, (\mathsf{SS.Rec}_P)_{P\subseteq[n]})$ represent a classical secret sharing scheme classified as [post-quantum computational, statistical, perfect] that realizes f. Thus, QASS represents a [computational, statistical, perfect] quantum anamorphic secret sharing scheme for f, with the*

total share size for the anamorphic secret is $= \mathsf{size}(\mathsf{QC.Enc}(M_f^{(1)})) + (4d_1+2d_2+1) + 6\lceil \log|\mathcal{R}|\rceil + \lceil \log|\mathcal{J}|\rceil + \lceil \log\big(2^{d_1+1}!\big)\rceil)$.

The difference between the anamorphic share size and the original share size, along with anamorphic key shares, is

$$\mathsf{size}\Big(\mathsf{QASS.Share}(M_f^{(1)}\Big) - \mathsf{size}\Big(\mathsf{QASS.Share}(M_f^{(0)})\Big) = 0.$$

Moreover, QASS exhibits efficient sharing and reconstruction protocols whenever QC and SS do.

Correctness and Privacy:

Theorem 15. *Let $P \subseteq [n]$ be an authorized set of players (i.e., $f(P) = 1$). Then the reconstruction procedure $\mathsf{QASS.Rec}_P(\sigma)$ applied to the sharing state $\mathsf{QASS.Share}(M_f^{(1)})$ correctly reconstructs the original message M_o and the covert message M_c. In other words, if*

$$\mathsf{QASS.Rec}_P(\sigma) := \Big(\mathsf{DOM}\big(\mathsf{QC.Rec}_P(\mathrm{Tr}_{\mathsf{key}_a}(\sigma))\big),\, \mathsf{DCM}\big(\mathsf{QC.Rec}_P(\mathrm{Tr}_{\mathsf{key}_a}(\sigma))\big)\Big),$$

then

$$\mathsf{QASS.Rec}_P(\sigma) = (M_o, M_c),$$

where M_o is the original message and M_c is the covert message.

Proof. We assume that both the classical secret sharing scheme SS and the quantum encoding scheme QC satisfy their correctness properties. The scheme distributes classical shares $s_i^{(a)}$ for each $i \in [n]$ corresponding to the keys $(k_1, k_2, k_3, k_4, k_5, k_6)$. By the correctness of the classical secret sharing scheme SS, if $P \subseteq [n]$ is an authorized set (i.e., $f(P) = 1$), then

$$\mathsf{SS.Rec}_P\Big(\{s_i^{(a)}\}_{i\in P}\Big) = (k_1, k_2, k_3, k_4, k_5, k_6). \tag{110}$$

The overall sharing state is given by

$$\sigma = \sum_{\vec{k},\,\vec{r}} \alpha(\vec{k}, \vec{r}) \left(\bigotimes_{i=1}^{6} \tau_{(k_i, r_i)}\right) \otimes \xi_{M_f^{(1)}},$$

where $\vec{k} = (k_1, k_2, k_3, k_4, k_5, k_6)$, $\vec{r} = (r_1, \ldots, r_6)$ and the normalization constant is

$$\alpha(\vec{k}, \vec{r}) = \frac{1}{2^{4d_1+2d_2+2}} \frac{1}{|\mathcal{R}|^6} \frac{1}{|\mathcal{J}|} \frac{1}{(2^{d_1+1})!}.$$

The subsystem corresponding to the classical key shares is denoted by key_a. By linearity of the trace and by the independence of the classical and quantum parts, we have

$$\mathrm{Tr}_{\mathsf{key}_a}(\sigma) = \xi_{M_f^{(1)}}. \tag{111}$$

The normalization factors in the definition of σ guarantee that $\sum_{\vec{k},\vec{r}} \alpha(\vec{k}, \vec{r}) = 1$, so that the partial trace exactly recovers the quantum component $\xi_{M_f^{(1)}}$.

Since $\xi_{M_f^{(1)}} = \mathsf{QC.Enc}(M_f^{(1)})$, the correctness of the quantum encoding scheme QC implies that the reconstruction procedure applied to the quantum subsystem yields the secret, i.e.,

$$\mathsf{QC.Rec}_{P\subseteq[n]}\Big(\mathrm{Tr}_{\mathsf{key}_a}(\sigma)\Big) = \mathsf{QC.Rec}_{P\subseteq[n]}\big(\xi_{M_f^{(1)}}\big) = M_f^{(1)}. \tag{112}$$

The decoding maps DOM and DCM are applied to the reconstructed quantum state $M_f^{(1)}$ to extract the original message M_o and the covert message M_c, respectively. That is,

$$\begin{aligned} \mathsf{DOM}\big(M_f^{(1)}\big) &= M_o, \\ \mathsf{DCM}\big(M_f^{(1)}\big) &= M_c. \end{aligned} \tag{113}$$

Hence, the overall reconstruction procedure yields

$$\begin{aligned} \mathsf{QASS.Rec}_P(\sigma) &= \Big(\mathsf{DOM}\big(\mathsf{QC.Rec}_P(\mathrm{Tr}_{\mathsf{key}_a}(\sigma))\big),\, \mathsf{DCM}\big(\mathsf{QC.Rec}_P(\mathrm{Tr}_{\mathsf{key}_a}(\sigma))\big)\Big) \\ &= \Big(\mathsf{DOM}\big(M_f^{(1)}\big),\, \mathsf{DCM}\big(M_f^{(1)}\big)\Big) \\ &= (M_o, M_c). \end{aligned} \tag{114}$$

proving the correctness of the quantum anamorphic secret-sharing scheme. □

Theorem 16. *The above quantum anamorphic secret-sharing scheme has perfect privacy.*

Proof. To prove the correctness of the secret-sharing scheme, we show the existence of a reconstruction function. Let $P \subseteq [n]$ with $f(P) = 0$, that is P is an unauthorized subset of players. Then,

$$\begin{aligned}
&\mathrm{Tr}_{\overline{P}}(\mathsf{QASS.Share}(M_f^{(1)})) \\
&= \mathrm{Tr}_{\overline{P}}\Bigg[\sum_{k_1\in\{0,1\}^{2d_1}} \sum_{k_4\in\{0,1\}^{2d_2}} \sum_{k_2\in\{1,\ldots,2^{d_1+1}\}} \sum_{k_5\in\{1,\ldots,2^{d_1+1}\}} \sum_{r_1,r_2,r_3,r_4,r_5,r_6\in\mathcal{R}} \sum_{k_3\in\mathrm{Sym}\,(2^{d_1+1})} \sum_{k_6\in\mathcal{J}} \\
&\quad \frac{1}{2^{4d_1+2d_2+2}} \frac{1}{|\mathcal{R}|^6} \frac{1}{|\ \mathcal{J}\ |} \frac{1}{(2^{d_1+1})!} \quad \Bigg[\bigotimes_{i=1}^{6} \tau_{(k_i,r_i)} \otimes \xi_{M_f^{(1)}}\Bigg]\Bigg] \\
&= \sum_{k_1\in\{0,1\}^{2d_1}} \sum_{k_4\in\{0,1\}^{2d_2}} \sum_{k_2\in\{1,\ldots,2^{d_1+1}\}} \sum_{k_5\in\{1,\ldots,2^{d_1+1}\}} \sum_{k_3\in\mathrm{Sym}\,(2_1^d+1)} \sum_{k_6\in\mathcal{J}} \\
&\mathrm{Tr}_{\overline{P}}\left[\frac{1}{2^{4d_1+2d_2+2}} \frac{1}{(2^{d_1+1})!} \frac{1}{|\ \mathcal{J}\ |}\xi_{M_f^{(1)}}\right] \quad \bigotimes_{i=1}^{6} \mathrm{Tr}_{\overline{P}}\left[\sum_{r_i\in\mathcal{R}} \frac{1}{|\mathcal{R}|}\tau_{(k_i,r_i)}\right] \\
&= \sum_{k_1\in\{0,1\}^{2d_1}} \sum_{k_4\in\{0,1\}^{2d_2}} \sum_{k_2\in\{1,\ldots,2^{d_1+1}\}} \sum_{k_5\in\{1,\ldots,2^{d_1+1}\}} \sum_{k_3\in\mathrm{Sym}\,(2_1^d+1)} \sum_{k_6\in\mathcal{J}} \mathrm{Tr}_{\overline{P}}\left[\frac{1}{2^{4d_1+2d_2+2}} \frac{1}{(2^{d_1+1})!} \frac{1}{|\ \mathcal{J}\ |}\xi_{M_f^{(1)}}\right] \otimes \mathrm{Tr}_{\overline{P}}(\sigma_P) \\
&= \mathrm{Tr}_{\overline{P}}\left[\mathsf{QC.Enc}\left(\sum_{k_1\in\{0,1\}^{2d_1}} \sum_{k_4\in\{0,1\}^{2d_2}} \sum_{k_2\in\{1,\ldots,2^{d_1+1}\}} \sum_{k_5\in\{1,\ldots,2^{d_1+1}\}} \sum_{k_3\in\mathrm{Sym}\,(2^{d_1}+1)} \sum_{k_6\in\mathcal{J}} \frac{1}{2^{4d_1+2d_2+2}} \frac{1}{(2^{d_1+1})!} \frac{1}{|\ \mathcal{J}\ |} M_f^{(1)}\right)\right] \otimes \mathrm{Tr}_{\overline{P}}(\sigma_P) \\
&= \mathrm{Tr}_{\overline{P}}\left(\mathsf{QC.Enc}(\sigma'_P)\right) \otimes \mathrm{Tr}_{\overline{P}}(\sigma_P).
\end{aligned} \tag{115}$$

Since the density matrix σ_P is only dependent upon the set of players P, the unauthorized set of players P cannot reconstruct the secret.

Next, We will show that if the SS is $\frac{\epsilon}{12}$-statistically private then the QASS is ϵ-statistically private. For any two keys $k, k' \in \{0,1\}^{2d_1} \times \{0,1\}^{2d_2} \times \{1,\dots,2^{d_1+1}\} \times \{1,\dots,2^{d_1+1}\} \times \mathrm{Sym}\,(2^{d_1+1}) \times \mathcal{J}$; where $k = (k_1, k_4, k_2, k_5, k_3, k_6)$ and $k' = (k'_1, k'_4, k'_2, k'_5, k'_3, k'_6)$.

For each $i = 1, \dots, 6$, the partial trace over subsystem $\overline{P}$ reduces to

$$\mathrm{Tr}_{\overline{P}}\left(\sum_{r_i \in \mathcal{R}} \frac{1}{|\mathcal{R}|} \tau_{(k_i, r_i)}\right) = \sum_{v_i} p^{(i)}_{v_i} \left|v_i\right\rangle \left\langle v_i\right|, \tag{116}$$

where for each $v = (v_1, \dots, v_6) \in \mathcal{S}_P$, $p^{(i)}_{v_i} = \Pr_{r_i \leftarrow \mathcal{R}}[\mathsf{Share}(k_i; r_i)_P = v_i]$ and $p^{(i)'}_{v_i} = \Pr_{r_i \leftarrow \mathcal{R}}[\mathsf{Share}(k'_i; r_i)_P = v_i]$ are defined to be the marginal probability distributions induced by the secret sharing process for k_i and k'_i on subsystem $\overline{P}$ and $\left|v_i\right\rangle \left\langle v_i\right|$ represents the basis state corresponding to v_i.

Then,

$$\mathrm{Tr}_{\overline{P}}\left[\bigotimes_{i=1}^{6}\left(\sum_{r_i \in \mathcal{R}} \frac{1}{|\mathcal{R}|} \tau_{(k_i, r_i)}\right)\right] = \sum_{v \in \mathsf{S}_P}\left(\prod_{i=1}^{6} p^{(i)}_{v_i}\right)\left[\bigotimes_{i=1}^{6} \left|v_i\right\rangle \left\langle v_i\right|\right] \quad = \sum_{v \in \mathsf{S}_P}\left(\prod_{i=1}^{6} p^{(i)}_{v_i}\right) \left|v\right\rangle \left\langle v\right|, \tag{117}$$

where $\bigotimes_{i=1}^{6} \left|v_i\right\rangle \left\langle v_i\right| = \left|v\right\rangle \left\langle v\right|$ and we get the following relation between the trace distance and the total variation distance

$$D\left(\mathrm{Tr}_{\overline{P}}\left[\bigotimes_{i=1}^{6}\left(\sum_{r_i \in \mathcal{R}} \frac{1}{|\mathcal{R}|} \tau_{(k_i, r_i)}\right)\right], \mathrm{Tr}_{\overline{P}}\left[\bigotimes_{i=1}^{6}\left(\sum_{r_i \in \mathcal{R}} \frac{1}{|\mathcal{R}|} \tau_{(k'_i, r_i)}\right)\right]\right) = D\left(\sum_{v \in \mathsf{S}_P} \prod_{i=1}^{6} p^{(i)}_{v_i} \left|v\right\rangle \left\langle v\right|, \sum_{v \in \mathsf{S}_P} \prod_{i=1}^{6} p^{(i)'}_{v_i} \left|v\right\rangle \left\langle v\right|\right) \tag{118}$$

$$\leq \Delta\left(\{\prod_{i=1}^{6} p^{(i)}_{v_i}\}_{v \in \mathsf{S}_P},\ \{\prod_{i=1}^{6} p^{(i)'}_{v_i}\}_{v \in \mathsf{S}_P}\right), \tag{119}$$

which we got using the Lemma 22. (Property v.).

Now we prove the privacy of the QASS. Let $P \subseteq [n]$ be an unauthorized subset such with $f(P) = 0$. For any two secret states $M^{(1)}_f$ and $M^{(1)'}_f$. Our argument is a hybrid one. First, we will contend that the perfect privacy of the one-time pad, along with Lemma 5, ensures that the composite shares of $\overline{P}$ for two secrets $M^{(1)}_f$ and $M^{(1)'}_f$ will be computationally indistinguishable. We define sharing of a random anamorphic key by

$$\kappa^{(a)} = \sum_{k'_1 \in \{0,1\}^{2d_1}} \sum_{k'_4 \in \{0,1\}^{2d_2}} \sum_{k'_2 \in \{1,\dots,2^{d_1+1}\}} \sum_{k'_5 \in \{1,\dots,2^{d_1+1}\}} \sum_{r_1, r_2, r_3, r_4, r_5, r_6 \in \mathcal{R}} \sum_{k'_3 \in \mathrm{Sym}\,(2^{d_1+1})} \sum_{k'_6 \in \mathcal{J}} \frac{1}{2^{4d_1+2d_2+2}} \frac{1}{|\mathcal{R}|^6} \frac{1}{\mid \mathcal{J} \mid} \frac{1}{2^{d_1+1}!}\left[\bigotimes_{i=1}^{6} \tau_{(k'_i, r_i)}\right]. \tag{120}$$

and we define the hybrids

$$\Psi_1 = \mathrm{Tr}_{\overline{P}}\left[\left(\sum_{k_1 \in \{0,1\}^{2d_1}} \sum_{k_4 \in \{0,1\}^{2d_2}} \sum_{k_2 \in \{1,\dots,2^{d_1+1}\}} \sum_{k_5 \in \{1,\dots,2^{d_1+1}\}} \sum_{k_3 \in \mathrm{Sym}\,(2^{d_1+1})} \frac{1}{2^{4d_1+2d_2+2}} \frac{1}{(2^{d_1+1})!} \xi_{M^{(1)}_f}\right) \otimes \kappa^{(a)}\right] \tag{121}$$

and

$$\Psi_2 = \mathrm{Tr}_{\overline{P}}\left[\left(\sum_{k_1 \in \{0,1\}^{2d_1}} \sum_{k_4 \in \{0,1\}^{2d_2}} \sum_{k_2 \in \{1,\dots,2^{d_1+1}\}} \sum_{k_5 \in \{1,\dots,2^{d_1+1}\}} \sum_{k_3 \in \mathrm{Sym}\,(2^{d_1+1})} \frac{1}{2^{4d_1+2d_2+2}} \frac{1}{(2^{d_1+1})!} \xi_{M^{(1)'}_f}\right) \otimes \kappa^{(a)}\right] \tag{122}$$

Our goal is to show $D(\Psi_1, \Psi_2) = 0$.

Subsequently, we will demonstrate that composite shares of the same secret are within a $\frac{\epsilon}{2}$-close trace distance when the shares of the key are replaced with shares of a random key, as opposed to when they are not replaced. We will show

$$D\left(\mathrm{Tr}_{\overline{P}}\left(\mathsf{QSS.Share}(M^{(1)}_f)\right), \Psi_1\right) \leq \frac{\epsilon}{2} \tag{123}$$

and

$$D(\mathrm{Tr}_{\overline{P}}(\Psi_2, \mathsf{QSS.Share}(M_f^{(1)'}))) \leq \frac{\epsilon}{2} \tag{124}$$

Then using the triangle inequality we will show that

$$D(\mathrm{Tr}_{\overline{P}}(\mathsf{QASS.Share}(M_f^{(1)})), \mathrm{Tr}_{\overline{P}}(\mathsf{QASS.Share}(M_f^{(1)'}))) \leq \epsilon \tag{125}$$

Using the [Property (ii), Lemma 22] and by distributing the partial trace we get

$$\begin{aligned} D(\Psi_1, \Psi_2) = D\Bigg(&\mathrm{Tr}_{\overline{P}}\Bigg[\sum_{k_1 \in \{0,1\}^{2d_1}} \sum_{k_4 \in \{0,1\}^{2d_2}} \sum_{k_2 \in \{1,\ldots,2^{d_1+1}\}} \sum_{k_5 \in \{1,\ldots,2^{d_1+1}\}} \sum_{k_3 \in \mathrm{Sym}(2^{d_1+1})} \frac{1}{2^{4d_1+2d_2+2}} \frac{1}{(2^{d_1+1})!} \xi_{M_f^{(1)}} \Bigg], \\ &\mathrm{Tr}_{\overline{P}}\Bigg[\sum_{k_1 \in \{0,1\}^{2d_1}} \sum_{k_4 \in \{0,1\}^{2d_2}} \sum_{k_2 \in \{1,\ldots,2^{d_1+1}\}} \sum_{k_5 \in \{1,\ldots,2^{d_1+1}\}} \sum_{k_3 \in \mathrm{Sym}(2^{d_1+1})} \frac{1}{2^{4d_1+2d_2+2}} \frac{1}{(2^{d_1+1})!} \xi_{M_f^{(1)'}} \Bigg] \Bigg) \end{aligned} \tag{126}$$

Therefore, when the key is chosen uniformly random, according to Lemma 5, the input is perfectly hidden by the quantum one-time pad and there exists a state ϑ such that

$$D(\Psi_1, \Psi_2) = D(\mathrm{Tr}_{\overline{P}}(\mathsf{QC.Enc}(\vartheta)), \mathsf{QC.Enc}(\vartheta))) = 0 \tag{127}$$

By the [Properties v. and iv., Lemma 22], we get,

$$\begin{aligned} &D(\Psi_1, \mathrm{Tr}_{\overline{P}}(\mathsf{QASS.Share}(M_f^{(1)}))) \\ &= D\Bigg(\sum_{k_1 \in \{0,1\}^{2d_1}} \sum_{k_4 \in \{0,1\}^{2d_2}} \sum_{k_2 \in \{1,\ldots,2^{d_1+1}\}} \sum_{k_5 \in \{1,\ldots,2^{d_1+1}\}} \sum_{k_3 \in \mathrm{Sym}\,(2^{d_1+1})} \frac{1}{2^{4d_1+2d_2+2}} \frac{1}{(2^{d_1+1})!} \mathrm{Tr}_{\overline{P}}(\xi_{M_f^{(1)}}) \otimes \mathrm{Tr}_{\overline{P}}(\kappa^{(a)}), \\ &\sum_{k_1 \in \{0,1\}^{2d_1}} \sum_{k_4 \in \{0,1\}^{2d_2}} \sum_{k_2 \in \{1,\ldots,2^{d_1+1}\}} \sum_{k_5 \in \{1,\ldots,2^{d_1+1}\}} \sum_{k_3 \in \mathrm{Sym}\,(2^{d_1+1})} \frac{1}{2^{4d_1+2d_2+2}} \frac{1}{(2^{d_1+1})!} \mathrm{Tr}_{\overline{P}}(\xi_{M_f^{(1)}}) \otimes \mathrm{Tr}_{\overline{P}}\Bigg[\bigotimes_{i=1}^{6} \Bigg(\sum_{r_i \in \mathcal{R}} \frac{1}{|\mathcal{R}|} \tau_{(k_i, r_i)} \Bigg) \Bigg] \Bigg) \\ &\leq \sum_{k_1 \in \{0,1\}^{2d_1}} \sum_{k_4 \in \{0,1\}^{2d_2}} \sum_{k_2 \in \{1,\ldots,2^{d_1+1}\}} \sum_{k_5 \in \{1,\ldots,2^{d_1+1}\}} \sum_{k_3 \in \mathrm{Sym}\,(2^{d_1+1})} \frac{1}{2^{4d_1+2d_2+2}} \frac{1}{(2^{d_1+1})!} \\ &D\Bigg(\mathrm{Tr}_{\overline{P}}(\kappa^{(a)}), \mathrm{Tr}_{\overline{P}}\Bigg[\bigotimes_{i=1}^{6} \Bigg(\sum_{r_i \in \mathcal{R}} \frac{1}{|\mathcal{R}|} \tau_{(k_i, r_i)} \Bigg) \Bigg] \Bigg) \end{aligned} \tag{128}$$

By using the Lemma 22 (Property i.), we get

$$\begin{aligned} &D(\Psi_1, \mathrm{Tr}_{\overline{P}}(\mathsf{QASS.Share}(M_f^{(1)}))) \\ &\leq \sum_{k_1, k_1' \in \{0,1\}^{2d_1}} \sum_{k_4, k_4' \in \{0,1\}^{2d_2}} \sum_{k_2, k_2' \in \{1,\ldots,2^{d_1+1}\}} \sum_{k_5, k_5' \in \{1,\ldots,2^{d_1+1}\}} \sum_{k_3, k_3' \in \mathrm{Sym}\,(2^{d_1+1})} \\ &\quad \frac{1}{4^{4d_1+2d_2+2}} \frac{1}{((2^{d_1+1})!)^2} D\Bigg(\mathrm{Tr}_{\overline{P}}\Bigg[\bigotimes_{i=1}^{6} \Bigg(\sum_{r_i \in \mathcal{R}} \frac{1}{|\mathcal{R}|} \tau_{(k_i', r_i)} \Bigg) \Bigg], \mathrm{Tr}_{\overline{P}}\Bigg[\bigotimes_{i=1}^{6} \Bigg(\sum_{r_i \in \mathcal{R}} \frac{1}{|\mathcal{R}|} \tau_{(k_i, r_i)} \Bigg) \Bigg] \Bigg) \\ &\leq \sum_{k_1, k_1' \in \{0,1\}^{2d_1}} \sum_{k_4, k_4' \in \{0,1\}^{2d_2}} \sum_{k_2, k_2' \in \{1,\ldots,2^{d_1+1}\}} \sum_{k_5, k_5' \in \{1,\ldots,2^{d_1+1}\}} \sum_{k_3, k_3' \in \mathrm{Sym}\,(2^{d_1+1})} \\ &\quad \frac{1}{4^{4d_1+2d_2+2}} \frac{1}{((2^{d_1+1})!)^2} \Delta\Bigg(\{\prod_{i=1}^{6} p_{v_i}^{(i)}\}_{v \in \mathsf{S}_P}, \{\prod_{i=1}^{6} p_{v_i}^{(i)'}\}_{v \in \mathsf{S}_P} \Bigg) \end{aligned} \tag{129}$$

If P and P' are two probability distributions over a finite set $\mathcal{S}_P$, then the statistical distance between two probability distributions P and P' is

$$\Delta(P, P') = \frac{1}{2} \sum_{v \in \mathsf{S}_P} |p_v - p_v'|. \tag{130}$$

Now, considering two product distributions formed from marginals

$$P = \left\{ \prod_{i=1}^{6} p_{v_i}^{(i)} \right\}_{v \in \mathsf{S}_P}, \quad P' = \left\{ \prod_{i=1}^{6} p_{v_i}^{(i)'} \right\}_{v \in \mathsf{S}_P}.$$

we get

$$\Delta(P, P') = \frac{1}{2} \sum_{v \in \mathsf{S}_P} \left| \prod_{i=1}^{6} p_{v_i}^{(i)} - \prod_{i=1}^{6} p_{v_i}^{(i)'} \right|. \tag{131}$$

Using the telescoping expansion of the difference

$$\prod_{i=1}^{6} p_{v_i}^{(i)} - \prod_{i=1}^{6} p_{v_i}^{(i)'} = \sum_{j=1}^{6} \left(\prod_{i=1}^{j-1} p_{v_i}^{(i)'} \right) \left(p_{v_j}^{(j)} - p_{v_j}^{(j)'} \right) \left(\prod_{i=j+1}^{6} p_{v_i}^{(i)} \right), \tag{132}$$

we get

$$\begin{aligned} \left| \prod_{i=1}^{6} p_{v_i}^{(i)} - \prod_{i=1}^{6} p_{v_i}^{(i)'} \right| &\leq \sum_{j=1}^{6} \left| \prod_{i=1}^{j-1} p_{v_i}^{(i)'} \cdot (p_{v_j}^{(j)} - p_{v_j}^{(j)'}) \cdot \prod_{i=j+1}^{6} p_{v_i}^{(i)} \right| \quad \text{(by the triangular inequality)} \\ &\leq \sum_{j=1}^{6} |p_{v_j}^{(j)} - p_{v_j}^{(j)'}| \quad \text{(since each probability lies in } [0,1]). \end{aligned} \tag{133}$$

Summing over all elements of $\mathcal{S}_P$ we get the statistical distance

$$\begin{aligned} \Delta(P, P') &= \frac{1}{2} \sum_{v \in \mathsf{S}_P} \left| \prod_{i=1}^{6} p_{v_i}^{(i)} - \prod_{i=1}^{6} p_{v_i}^{(i)'} \right| \\ &\leq \frac{1}{2} \sum_{v \in \mathsf{S}_P} \sum_{j=1}^{6} |p_{v_j}^{(j)} - p_{v_j}^{(j)'}| \\ &= \frac{1}{2} \sum_{j=1}^{6} \sum_{v \in \mathsf{S}_P} |p_{v_j}^{(j)} - p_{v_j}^{(j)'}| \quad \text{(as both sums are finite)} \\ &= \sum_{j=1}^{6} \Delta(p^{(j)}, p^{(j)'}). \end{aligned} \tag{134}$$

Given for each $j = 1, \ldots, 6$, $\Delta(p^{(j)}, p^{(j)'}) \leq \frac{\epsilon}{12}$, for some $\epsilon > 0$, we have

$$\Delta(P, P') = \Delta \left(\left\{ \prod_{i=1}^{6} p_{v_i}^{(i)} \right\}_{v \in \mathcal{S}_P}, \left\{ \prod_{i=1}^{6} p_{v_i}^{(i)'} \right\}_{v \in \mathcal{S}_P} \right) \leq 6 \left(\frac{\epsilon}{12} \right) = \frac{\epsilon}{2}. \tag{135}$$

This is the statistical distance between the classical sharing of keys k, k'. Therefore, invoking $\frac{\epsilon}{12}$-statistical privacy of SS and Equation 129, we get

$$D(\Psi_1, \mathrm{Tr}_{\overline{P}}(\mathsf{QASS}(M_f^{(1)}))) \leq \frac{\epsilon}{2}. \tag{136}$$

In a similar way we can prove that

$$D(\Psi_2, \mathrm{Tr}_{\overline{P}}(\mathsf{QASS}(M_f^{(1)'}))) \leq \frac{\epsilon}{2}. \tag{137}$$

Therefore,

$$\begin{aligned} & D(\mathrm{Tr}_{\overline{P}}(\mathsf{QASS.Share}(M_f^{(1)})), \mathrm{Tr}_{\overline{P}}(\mathsf{QASS.Share}(M_f^{(1)'}))) \\ & \leq D(\Psi_1, \mathrm{Tr}_{\overline{P}}(\mathsf{QASS}(M_f^{(1)}))) + D(\Psi_1, \Psi_2) + D(\Psi_2, \mathrm{Tr}_{\overline{P}}(\mathsf{QASS}(M_f^{(1)'}))) \\ & \leq \frac{\epsilon}{2} + 0 + \frac{\epsilon}{2} \\ & = \epsilon \end{aligned} \tag{138}$$

Since $\epsilon > 0$ is arbitrary, $D(\mathrm{Tr}_{\overline{P}}(\mathsf{QASS.Share}(M_f^{(1)})), \mathrm{Tr}_{\overline{P}}(\mathsf{QASS.Share}(M_f^{(1)'}))) = 0$. Hence, the quantum anamorphic secret sharing scheme has perfect privacy.

Following the proof idea from Theorem 9., page 22, in the paper [20], we can prove the computational privacy similarly by replacing the trace distance with the quantum advantage pseudometric $\mathsf{Adv}_{\mathcal{F}}(\rho, \sigma)$ 4, and properties in Lemma 23. □

It is important to note that this compiler can be extended to accommodate states of any arbitrary dimension [20]. It is essential to assume that f', and consequently f, adheres to the no-cloning property $f(P) = 1 \implies f(\overline{P}) = 0$, so that an appropriate QECC can be applied [20]. As in the paper [20] Çakan et al. noted that we can take any quantum erasure-correcting code QC realizing any monotone function f' with $f' \geq f$, and this means even when we do not know efficient QECCs for f, we may take some $f' \geq f$ to use an efficient QECC.

Let T_n^t be the t-out-of-n threshold function such that $T_n^t(P) = 1$ iff $\mid P \mid \geq t$, then $T_n^t \geq f$. As we have seen above choosing a correct f' is important and here for the choice of threshold function, we may take $f' = T_n^t$ [20].

The following results are from the paper [20] from Section 5. and Section 6. These results are applicable in our work and the share sizes can be computed based on these results. You have included them to mention the existing works on existence of post quantum computational classical secret-sharing scheme realizing f and construction of f'.

We use the compiler we have constructed to design efficient computational quantum anamorphic secret-sharing schemes. The following lemma is due to Yao [37] and Cleve, Gottesman, and Lo [75].

Lemma 17. *([37], [75]) If f belongs to* monotone P*, then an efficient post-quantum computational classical secret-sharing scheme realizing f can be constructed, assuming the existence of post-quantum secure one-way functions.*

Lemma 18. *(Quantum Shamir secret sharing [76]) For any $t > n/2$, there exists an efficient perfect quantum secret sharing scheme that realizes T_n^t with a share size of $O(n \log n)$.*

The following theorem is due to Çakan et al..

Theorem 19. *([20]) If f is a heavily monotone function within* monotone P*, then an efficient computational quantum secret-sharing scheme can be constructed to realize f, assuming the existence of post-quantum secure one-way functions.*

In the proof [Theorem 11., Page 25., [20]] for $t = \lfloor \frac{n}{2} \rfloor + 1$, $f' = T_n^t$ is chosen for which $T_n^t \geq f$, when f is heavy.

Definition 30. *([20]) A monotone function f is said to be in* mNP *if the corresponding language $\mathcal{L} = \{x \in \{0,1\}^n \mid f(x) = 1\}$ is in* NP.

Let $n \in \mathbb{Z}^+$ be a positive integer representing the number of players. Define $\mathcal{S}$ as the Hilbert space corresponding to the secret space. Let $\mathcal{H}_1, \ldots, \mathcal{H}_n$ be Hilbert spaces representing the share spaces for the n players. Consider $f\colon \{0,1\}^n \longrightarrow \{0,1\}$ as a no-cloning monotone function that characterizes a language $\mathcal{L} \in$ mNP, and let $\mathcal{Y}$ be a polynomial-time verifier for $\mathcal{L}$.

Anamologous to the definition of the quantum secret-sharing(QSS) in mNP from [Section 6, Page 26., [20]], we can define the QASS too.

Definition 31. *([20]) A quantum anamorphic secret-sharing scheme (*QASS*) for* mNP *that realizes an access function f is defined as a set of trace-preserving quantum operations:*

$$\Sigma_{\mathsf{QASS}}^{\mathsf{mNP}} = (\mathsf{QASS.Share}, (\mathsf{QASS.Rec}_{P \subseteq [n]}^{\mathsf{AM}}))$$

that satisfy the following conditions for all subsets $P \subseteq [n]$:

- ***Correctness**: If $f(P) = 1$, then for any valid witness w such that $\mathcal{Y}(P, w) = 1$, the reconstruction process ensures that if ρ_P represents the shares held by the subset P, then*

$$\mathsf{Rec}_P(\rho_P, P, w) = |\psi\rangle.$$

- ***Privacy**: If $f(P) = 0$, then for any quantum states $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{S}$ and for any quantum polynomial-time (QPT) adversary $\{C_\lambda\}_\lambda$, the following holds:*

$$|\Pr\big[C(\mathrm{Tr}_{\overline{P}}(\mathsf{Share}(|\psi_1\rangle\langle\psi_1|; 1^\lambda))) = 1\big] - \Pr\big[C(\mathrm{Tr}_{\overline{P}}(\mathsf{Share}(|\psi_2\rangle\langle\psi_2|; 1^\lambda))) = 1\big]| \leq \mathsf{negl}(\lambda).$$

Lemma 20. *([39]) If $f \in$ mNP, there is an efficient post-quantum computational classical secret-sharing scheme realizing f based on the existence of post quantum secure witness encryption for* NP *and one-way functions.*

The following theorem is proved by Çakan et al. [Section 6, Page 26, Theorem 12] proving the existence of a QSS for every heavy function in mNP.

Theorem 21. *[20] For any heavy function $f\colon \{0,1\} \longrightarrow \{0,1\}$ belonging to* mNP*, there exists a computational* QSS *that realizes f with* size(QSS) *bounded above by* poly(n)*. This construction relies on the existence of post-quantum secure witness encryption for* NP *and the existence of one-way functions.*

Consequently, the existence of $\Sigma^{\mathsf{mNP}}_{\mathsf{QASS}}$ can be shown easily by exactly following and extending the compiler, as we have constructed in Theorem 14 with similar $f' = T^{\lfloor \frac{n}{2} \rfloor} + 1$ [Theorem 12., Page 26, [20]].

VIII. Discussions

A. Qubit Requirements and Entropy Computations

• **Total number of qubits:** The anamorphic ciphertext $M_f^{(1)}$ and the original ciphertext $M_f^{(o)}$, both resides in the Hilbert space $(\mathbb{C}^2)^{\otimes(d_1+1)}$. Therefore the anamorphic encryption requires (d_1+1) qubits. Processing $M_f^{(1)}$ also requires (d_1+1) qubits. Extracted messages M_o and M_c use d_1 and d_2 qubits, respectively, but the decryption circuit operates on (d_1+1) qubits.

• **Mutual informations, von-Neumann entropy and relative entropy:** We have defined the original ciphertext $M_f^{(0)} = \sigma_l M_a^{(0)} \sigma_l^\dagger$, where

$$M_a^{(0)} = \begin{pmatrix} \frac{1}{2}M_o' & 0 \\ 0 & \frac{1}{2}M_o' \end{pmatrix}.$$

Because σ_l is unitary, the spectrum of $M_f^{(0)}$ is unchanged.

let $\{\lambda_i\}_{i=1}^{2^{d_1}}$ be the eigenvalues of the original quantum density matrix M_o and since M_o' is obtained by using QOTP, the eigenvalues of the M_o' is same as the eigenvalues of M_o.

Thus the von Neumann entropy of $M_f^{(0)}$ is

$$\begin{aligned}
\mathsf{S}(M_f^{(0)}) &= -\sum_{i=1}^{2^{d_1}} \Big[2\Big(\frac{1}{2}\lambda_i\Big)\ \log\Big(\frac{1}{2}\lambda_i\Big)\Big] \\
&= -\sum_{i=1}^{2^{d_1}} \lambda_i \Big[\log(\lambda_i) - \log 2\Big] \\
&= -\sum_{i=1}^{2^{d_1}} \lambda_i \log \lambda_i \ + \ \sum_{i=1}^{2^{d_1}} \lambda_i \\
&= \mathsf{S}(M_o') + 1, \qquad\qquad (\text{since } \mathrm{Tr}(M_o) = 1).
\end{aligned}$$

Therefore, $\mathsf{S}(M_f^{(0)}) = \mathsf{S}(M_o') + 1$

We compute $\mathsf{S}(M_f^{(1)})$ for a particular case, assuming that both M_o' and M_c'' are are simultaneously diagonalizable. Let $\{\mu_i\}_{i=1}^{2^{d_1}}$ be the eigenvalues of the embedded covert quantum density matrix M_c''.

Thus for each $i = 1, \ldots, 2^{d_1+1}$, we get pair of eigenvalues of $M_f^{(1)}$ as $\Big\{\frac{1}{2}\lambda_i \pm \frac{1}{\eta}\,\mu_i\Big\}$, since M_o is strictly positive-definite. Then,

$$\mathsf{S}(M_f^{(1)}) = -\sum_{i=1}^{2^{d_1+1}} \left[\Big(\frac{1}{2}\lambda_i + \frac{1}{\eta}\,\mu_i\Big)\log\Big(\frac{1}{2}\lambda_i + \frac{1}{\eta}\,\mu_i\Big) + \Big(\frac{1}{2}\lambda_i - \frac{1}{\eta}\,\mu_i\Big)\log\Big(\frac{1}{2}\lambda_i - \frac{1}{\eta}\,\mu_i\Big)\right].$$

As QOTP encryption is information-theoretically secure. In other words, if the keys are unknown then the ciphertext reveals no information about the underlying plaintext. In our construction the states M_o' and M_c' are encrypted by independent random QOTP keys, so that without knowledge of the key one has

$$I(M_o; M_f^{(1)}) = 0 \quad \text{and} \quad I(M_c; M_f^{(1)}) = 0.$$

We now compute the quantum relative entropy for a particular case, under the same assumption that M_o' and M_c'' are simultaneously diagonalizable

$$\begin{aligned}
S(M_f^{(1)} \| M_f^{(0)}) &= \sum_{i=1}^{2^{d_1+1}} \left[\Big(\frac{1}{2}\lambda_i + \frac{1}{\eta}\,\mu_i\Big)\log\frac{\frac{1}{2}\lambda_i + \frac{1}{\eta}\,\mu_i}{\frac{1}{2}\lambda_i} + \Big(\frac{1}{2}\lambda_i - \frac{1}{\eta}\,\mu_i\Big)\log\frac{\frac{1}{2}\lambda_i - \frac{1}{\eta}\,\mu_i}{\frac{1}{2}\lambda_i}\right] \\
&= \sum_{i=1}^{2^{d_1+1}} \left[\Big(\frac{1}{2}\lambda_i + \frac{1}{\eta}\,\mu_i\Big)\log\Big(1 + \frac{2\,\mu_i}{\eta\,\lambda_i}\Big) + \Big(\frac{1}{2}\lambda_i - \frac{1}{\eta}\,\mu_i\Big)\log\Big(1 - \frac{2\,\mu_i}{\eta\,\lambda_i}\Big)\right].
\end{aligned}$$

Let $x_i = \frac{2\mu_i}{\eta\,\lambda_i}$, then

$$S(M_f^{(1)} \| M_f^{(0)}) = \sum_{i=1}^{2^{d_1+1}} \frac{1}{2}\lambda_i\Big[(1+x_i)\log_2(1+x_i) + (1-x_i)\log_2(1-x_i)\Big]. \tag{139}$$

Define the function

$$f(x) = \frac{1}{2}\Big[(1+x)\log_2(1+x) + (1-x)\log_2(1-x)\Big],$$

so that

$$S(M_f^{(1)} \| M_f^{(0)}) = \sum_{i=1}^{2^{d_1+1}} \lambda_i\, f(x_i).$$

For $|x| < 1$ and using the Taylor series expansion for the base-2 logarithm, we get,

$$f(x) = \frac{x^2}{2\ln 2} + \frac{x^4}{12\ln 2} + O(x^6). \tag{140}$$

The function $f(x)$ is *even* and *convex* in $(-1,1)$ and easy to verify that $f(x) \le x^2 \quad \text{for } |x| \le 1$.

Thus, for each i we have

$$\lambda_i\, f(x_i) \le \lambda_i\, x_i^2 = \lambda_i\, \left(\frac{2\mu_i}{\eta\,\lambda_i}\right)^2 = \frac{4\,\mu_i^2}{\eta^2\,\lambda_i}.$$

Thus we get

$$S(M_f^{(1)} \| M_f^{(0)}) \le \frac{4}{\eta^2} \sum_{i=1}^{2^{d_1+1}} \frac{\mu_i^2}{\lambda_i}.$$

As, $\frac{1}{\eta} < \mathsf{negl}(\lambda)$, this bound indicates that in our construction the anamorphic ciphertext $M_f^{(1)}$ and the original ciphertext $M_f^{(0)}$ are indistinguishable.

B. Possible Attacks

In this section, we present two possible attacks by the dictator and discuss how they can be prevented.

Case-I: The adverary or the dictator is authorized to have the origianl key shares but not authorized to have covert key shares. As we proved the perfect privacy of both SS and ASS, the dictator cannot reconstruct the covert key shares but will be able to reconstruct the original key shares.

Case-II: If $\mathcal{D}$ *wants to enter as an extra player in the set of players to receive shares*. If the dictator joins the set of players as an additional player to obtain a share and subsequently demands that the authorized set of players submit their shares for message reconstruction, the authorized set of players strategically *partially cheats* the dictator. Specifically, while they provide the dictator with the correct key shares necessary to reconstruct the original message, they simultaneously submit *forged shares* for the other covert keys, thereby ensuring that the dictator is unable to access unauthorized information.

We now compute the Partial cheating probability $\mathsf{Cheat}^{(p)}\left(V_{i_1}^{(a)}, \ldots, V_{i_t}^{(a)}\right)$. In our construction, the anamorphic key is $k = (k_1, k_4, k_2, k_5, k_3, k_6)$, with the original key part $\mathsf{k}^{(o)} = (k_1, k_2, k_3)$ and the covert key part $\mathsf{k}^{(c)} = (k_4, k_5, k_6)$. The key is chosen uniformly at random from $\{0,1\}^{2d_1} \times \{0,1\}^{2d_2} \times \{1,\ldots,2^{d_1+1}\} \times \{1,\ldots,2^{d_1+1}\} \times \mathrm{Sym}(2^{d_1+1}) \times \mathcal{J}$. Thus, the covert key is uniformly distributed over $\mathcal{S}^{(c)} = \{0,1\}^{2d_2} \times \{1,\ldots,2^{d_1+1}\} \times \mathcal{J}$ with $|\ \mathcal{S}^{(c)}\ | = 2^{2d_2} \cdot 2^{d_1+1} \cdot |\mathcal{J}|$.

Suppose the honest covert shares of the t players (when they are honest) are $b^{(c)} = \left(s_{i_1}^{(c)}, s_{i_2}^{(c)}, \ldots, s_{i_t}^{(c)}\right)$, and the dictator's reconstruction function $\mathsf{Sec}^{(c)}$ then returns $\mathsf{Sec}^{(c)}(b^{(c)}) = s^{(c)}$, which is the (correct) covert secret.

Now, assume that a coalition of cheaters wishes to *partially cheat* by forging their covert shares. That is, they replace $b^{(c)}$ by some $b^{(c)'}$ with $b^{(c)'} \neq b^{(c)}$ (with at least one coordinate changed) while leaving the original part untouched (so that the overall reconstructed secret is $\mathsf{Sec}^{(p)}(b') = (\mathsf{Sec}^{(o)}(b), \mathsf{Sec}^{(c)}(b'))$ with $\mathsf{Sec}^{(o)}(b) = s^{(o)}$ as before). In our construction, since the key (and hence the covert secret) is chosen uniformly at random from $\mathcal{S}^{(c)}$ and the reconstruction function $\mathsf{Sec}^{(c)}$ is deterministic and surjective onto $\mathcal{S}^{(c)}$, any *forged* share tuple $b^{(c)'}$ will, in effect, cause the dictator to compute a covert secret that is uniformly distributed over $\mathcal{S}^{(c)}$. Since the forged reconstruction $\mathsf{Sec}^{(c)}(b^{(c)'})$ is uniform over $\mathcal{S}^{(c)}$, the probability that it accidentally equals the honest secret $s^{(c)}$ is

$$\Pr\Big(\mathsf{Sec}^{(c)}(b^{(c)'}) = s^{(c)}\Big) = \frac{1}{|\mathcal{S}^{(c)}|}.$$

Hence, the probability that the dictator reconstructs a covert secret different from $s^{(c)}$ (i.e. that the cheating is successful) is

$$\Pr\Big(\mathsf{Sec}^{(c)}(b^{(c)'}) \neq s^{(c)}\Big) = \Big(1 - \frac{1}{|\mathcal{S}^{(c)}|}\Big).$$

Since the cheating probability is defined as the maximum (over all possible true covert shares $b^{(c)}$ and over all feasible forged choices $b^{(c)'}$) of the above probability, we have

$$\mathsf{Cheat}^{(p)} \leq \Big(1 - \frac{1}{|\mathcal{S}^{(c)}|}\Big). \tag{141}$$

$$= \Big(1 - \frac{1}{2^{2d_2+d_1+1} \cdot |\mathcal{J}|}\Big), \tag{142}$$

which ensures the partial cheating probability is very high, and therefore the dictator cannot get the covert key shares with a very high probability. In fact, with optimal forging the players can achieve exactly this probability and the maximum cheating probability is equal to

$$\Big(1 - \frac{1}{2^{2d_2+d_1+1} \cdot |\mathcal{J}|}\Big). \tag{143}$$

IX. Conclusion

In this paper, we have constructed a quantum symmetric-key anamorphic encryption scheme and an anamorphic secret-sharing scheme. For future work, we aim to explore the following problems:

Question 1: Construct a quantum anamorphic public-key encryption (QAPKE) scheme.

Question 2: Develop quantum anamorphic secret-sharing using pseudorandom function-like state generators (PRFS) and optimize the share size in the case of anamorphic secret-sharing.

Acknowledgments

The authors are grateful to Goutam Mukherjee for his invaluable guidance, insightful discussions, and generous support throughout the preparation of this manuscript. We are thankful to TCG CREST and RKMVERI, Belur for generous research support.

X. Appendix

We have included useful results and properties in this section for use throughout our paper. Most of these results are taken from [48] and from the Appendix section of the paper [20].

Lemma 22. *(Trace distance [20], [48])*
i. For a probability distribution $\{p_i\}_{i\in I}$ and an ensembles of states $\{\rho_i\}_{i\in I}$

$$D(\sum_{i\in I} p_i\rho_i, \sigma) \leq \sum_{i\in I} p_i D(\rho_i, \sigma_i).$$

ii. For any trace-preserving quantum operation $\mathcal{E}$,

$$D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq D(\rho, \sigma).$$

iii. Let AB be a composite system and The states are assumed to be of AB,

$$D(\rho^A, \sigma^A) \leq D(\rho^{AB}, \sigma^{AB}).$$

iv. Given two density matrices σ and ρ, and for any state τ,

$$D(\rho \otimes \tau, \sigma \otimes \tau) = D(\rho, \sigma).$$

v. For any two probability distributions $\{p_i\}_{i\in I}$, $\{p'_i\}_{i\in I}$ and ensembles of states $\{\rho_i\}_{i\in I}$, $\{\sigma_i\}_{i\in I}$.

$$D\left(\sum_{i\in I} p_i\rho_i, \sum_{i\in I} p'_i\sigma_i\right) \leq \Delta(p_i, p'_i) + \sum_{i\in I} p_i D(\rho_i, \sigma_i).$$

vi. For any two states τ_1, τ_2,

$$D(\rho \otimes \tau_1, \sigma \otimes \tau_2) \leq D(\rho, \sigma) + D(\tau_1, \tau_2).$$

Proof. For the proofs see Section 9.2.1 of [48] and Appendix A of [20]. □

Lemma 23. *(Properties of Adversarial Advantage Pseudometric [20], [48])*
For any circuit family $\mathcal{F}$ and two states ρ, σ, the following holds:
i. $A_{\mathcal{F}}(\rho, \rho) = 0$;
ii. $A_{\mathcal{F}}(\rho, \sigma) = A_{\mathcal{F}}(\sigma, \rho)$;

iii. For any state τ,

$$A_{\mathcal{F}}(\rho,\sigma) \leq A_{\mathcal{F}}(\rho,\tau) + A_{\mathcal{F}}(\tau,\sigma);$$

iv. Assuming the states are of a composite system AB,

$$A_{\mathcal{F}}(\rho_A \otimes |0\rangle\langle 0|, \sigma_A \otimes |0\rangle\langle 0|) \leq A_{\mathcal{F}}(\rho_{AB}, \sigma_{AB});$$

v. For any two probability distributions, $\{p_i\}_{i\in I}$, $\{q_i\}_{i\in I}$, and ensembles of states $\{\rho_i\}_{i\in I}$, $\{\sigma_i\}_{i\in I}$,

$$A_{\mathcal{F}}\left(\sum_{i\in I} p_i\rho_i, \sum_{i\in I} q_i\sigma_i\right) \leq \Delta(p_i,q_i) + \sum_{i\in I} p_i A_{\mathcal{F}}(\rho_i,\sigma_i);$$

vi. For a probability distribution $\{p_i\}_{i\in I}$ and an ensemble of states $\{\rho_i\}_{i\in I}$,

$$A_{\mathcal{F}}\left(\sum_{i\in I} p_i\rho_i, \sigma\right) \leq \sum_{i\in I} p_i A_{\mathcal{F}}(\rho_i,\sigma);$$

vii. For any family $\mathcal{F}'$ and state τ such that there is $C' \in \mathcal{F}'$ satisfying $C'(\rho) = C(\rho\otimes\tau)$ and $C'(\sigma) = C(\sigma\otimes\tau)$ for any $C \in \mathcal{F}$,

$$A_{\mathcal{F}}(\rho\otimes\tau, \sigma\otimes\tau) \leq A_{\mathcal{F}'}(\rho,\sigma).$$

Proof. For the proofs see Appendix A of [20]. □

References

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[2] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 1996, pp. 212–219.

[3] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, p. 7–11, 1984.

[4] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*. Cambridge university press, 2010.

[5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, p. 145–195, 2002.

[6] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, no. 5410, p. 2050–2056, 1999.

[7] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, 1982.

[8] H. J. Kimble, "The quantum internet," *Nature*, vol. 453, p. 1023–1030, 2008.

[9] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, "Quantum computers," *Nature*, vol. 464, p. 45–53, 2010.

[10] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, 2018.

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

[12] D. Catalano, E. Giunta, and F. Migliaro, "Anamorphic encryption: New constructions and homomorphic realizations," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2024, pp. 33–62.

[13] F. Banfi, K. Gegier, M. Hirt, U. Maurer, and G. Rito, "Anamorphic encryption, revisited," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2024, pp. 3–32.

[14] R. Anderson and F. A. P. Petitcolas, "Limits on the effectiveness of steganography," in *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, 1998, pp. 474–481.

[15] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer*, vol. 35, no. 2, pp. 26–34, 2001.

[16] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge University Press, 2009.

[17] F. A. P. Petitcolas, R. Anderson, and M. G. Kuhn, "Information hiding: A survey," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062–1078, 1999.

[18] S. Katzenbeisser and F. A. P. Petitcolas, *Information Hiding: Techniques for Steganography and Digital Watermarking*. Artech House, 2000.

[19] R. Chandramouli and N. Memon, "Analysis of lsb based image steganography techniques," *Proceedings of IEEE International Conference on Image Processing*, vol. 3, pp. 1025–1028, 2002.

[20] A. Çakan, V. Goyal, C.-D. Liu-Zhang, and J. Ribeiro, "Computational quantum secret sharing," *arXiv preprint arXiv:2305.00356*, 2023.

[21] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, 1982.

[22] M. Girling, C. Cirstoiu, and D. Jennings, "Simple formulation of no-cloning and no-hiding that admits efficient and robust verification," *Physical Review Research*, 2024.

[23] D. Gottesman, "Theory of quantum secret sharing," *Physical Review A*, vol. 61, p. 042311, 1999.

[24] Z.-c. Yu, "The improved quantum secret sharing protocol based on grover algorithm," *Journal of Physics: Conference Series*, 2022.

[25] A. Cakan and V. Goyal, "Unclonable cryptography with unbounded collusions," *IACR Cryptology ePrint Archive*, 2023.

[26] Y. Li, "A kind of (n,t)threshold quantum state sharing scheme based on chinese reminder theorem," *Advances in Engineering Technology Research*, 2024.

[27] D. Catalano, E. Giunta, and F. Migliaro, "Generic anamorphic encryption, revisited: New limitations and constructions," *Cryptology ePrint Archive*, 2024.

[28] ——, "Limits of black-box anamorphic encryption," *Cryptology ePrint Archive*, 2024.

[29] M. Kutylowski, G. Persiano, D. H. Phan, M. Yung, and M. Zawada, "The self-anti-censorship nature of encryption: On the prevalence of anamorphic cryptography," *Cryptology ePrint Archive*, 2023.

[30] J. Jaeger and R. Stracovsky, "Dictators? friends? forgers." in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2025, pp. 105–137.

[31] Y. Wang, R. Chen, X. Huang, and M. Yung, "Sender-anamorphic encryption reformulated: Achieving robust and generic constructions," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2023, pp. 135–167.

[32] T. Okamoto, K. Tanaka, and S. Uchiyama, "Quantum public-key cryptosystems," in *Annual international cryptology conference*. Springer, 2000, pp. 147–165.

[33] K. Barooti, A. B. Grilo, L. Huguenin-Dumittan, G. Malavolta, O. Sattath, Q.-H. Vu, and M. Walter, "Public-key encryption with quantum keys," in *Theory of Cryptography Conference*. Springer, 2023, pp. 198–227.
[34] A. Beimel, "Secret-sharing schemes: A survey," in *Coding and Cryptology: Third International Workshop, IWCC 2011, Qingdao, China, May 30-June 3, 2011. Proceedings 3*. Springer, 2011, pp. 11–46.
[35] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.
[36] G. R. Blakley, "Safeguarding cryptographic keys," in *Managing requirements knowledge, international workshop on*. IEEE Computer Society, 1979, pp. 313–313.
[37] A. C.-C. Yao, "How to generate and exchange secrets," *Proceedings of the 27th Annual Symposium on Foundations of Computer Science*, p. 162–167, 1989.
[38] V. Vinod, A. Narayanan, K. Srinathan, C. P. Rangan, and K. Kim, "On the power of computational secret sharing," in *Progress in Cryptology-INDOCRYPT 2003: 4th International Conference on Cryptology in India, New Delhi, India, December 8-10, 2003. Proceedings 4*. Springer, 2003, pp. 162–176.
[39] R. Komargodski, M. Naor, and E. Yogev, "Secret sharing for np," in *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, 2014, p. 515–524.
[40] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Physical Review A*, vol. 59, pp. 1829–1834, 1999.
[41] A. Karlsson, M. Koashi, and N. Imoto, "Quantum entanglement for secret sharing and secret splitting," *Physical Review A*, vol. 59, pp. 162–168, 1999.
[42] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," *Physical Review Letters*, vol. 83, pp. 648–651, 1999.
[43] D. Gottesman, "Theory of quantum secret sharing," *Phys. Rev. A*, vol. 61, p. 042311, Mar 2000.
[44] A. Smith, "Quantum secret sharing and monotone span programs," *Journal of Cryptographic Security*, vol. 18, no. 7, p. 798–823, 2000.
[45] H. Imai, J. Müller-Quade, A. C. Nascimento, P. Tuyls, and A. Winter, "A quantum information theoretical model for quantum secret sharing schemes," *arXiv preprint quant-ph/0311136*, 2003.
[46] A. D. Smith, "Quantum secret sharing for general access structures," *arXiv preprint quant-ph/0001087*, 2000.
[47] W. Ogata, K. Kurosawa, D. R. Stinson, and H. Saido, "New combinatorial designs and their applications to authentication codes and secret sharing schemes," *Discrete Mathematics*, vol. 279, no. 1-3, pp. 383–405, 2004.
[48] M. A. Nielsen and I. L. Chuang, "Quantum computation and quantum information," *Phys. Today*, vol. 54, no. 2, p. 60, 2001.
[49] M. M. Wilde, *Quantum Information Theory*, 2nd ed. Cambridge University Press, 2017.
[50] M.-D. Choi, "Completely positive linear maps on complex matrices," *Linear Algebra and its Applications*, vol. 10, no. 3, pp. 285–290, 1975.
[51] B. Schumacher, "Quantum coding," *Physical Review A*, vol. 51, no. 4, p. 2738, 1995.
[52] A. Wehrl, *General Properties of Entropy*. American Physical Society, 1978, vol. 50, no. 2.
[53] D. A. Levin, Y. Peres, and E. L. Wilmer, *Markov Chains and Mixing Times*. American Mathematical Society, 2009.
[54] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Wiley-Interscience, 2006.
[55] P. Billingsley, *Probability and Measure*, 3rd ed. John Wiley & Sons, 1995.
[56] A. L. Gibbs and F. E. Su, "On choosing and bounding probability metrics," *International Statistical Review*, vol. 70, no. 3, pp. 419–435, 2002.
[57] C. A. Fuchs and J. van de Graaf, "Cryptographic distinguishability measures for quantum-mechanical states," *IEEE Transactions on Information Theory*, vol. 45, no. 4, pp. 1216–1227, 1999.
[58] A. Uhlmann, "The "transition probability" in the state space of a *-algebra," *Reports on Mathematical Physics*, vol. 9, no. 2, pp. 273–279, 1976.
[59] R. Jozsa, "Fidelity for mixed quantum states," *Journal of Modern Optics*, vol. 41, no. 12, pp. 2315–2323, 1994.
[60] R. A. Horn and C. R. Johnson, *Matrix analysis*. Cambridge university press, 2012.
[61] A. Ben-Israel and T. N. E. Greville, *Generalized Inverses: Theory and Applications*, 2nd ed. Springer, 2003.
[62] R. Penrose, "A generalized inverse for matrices," *Proceedings of the Cambridge Philosophical Society*, vol. 51, pp. 406–413, 1955.
[63] M. Keyl, "Fundamentals of quantum information theory," *Physics Reports*, vol. 369, no. 5, pp. 431–548, 2002. [Online]. Available: https://www.math.uci.edu/~brusso/keylphysrep.pdf
[64] G. Chiribella, "On quantum estimation, quantum cloning and finite quantum de finetti theorems," in *Theory of Quantum Computation, Communication, and Cryptography*, ser. Lecture Notes in Computer Science, vol. 6519. Springer, 2011, pp. 9–25. [Online]. Available: https://arxiv.org/abs/1010.1875
[65] W. Fulton and J. Harris, *Representation theory: a first course*. Springer Science & Business Media, 2013, vol. 129.
[66] J.-P. Serre *et al.*, *Linear representations of finite groups*. Springer, 1977, vol. 42.
[67] A. Ambainis, M. Mosca, A. Tapp, and R. De Wolf, "Private quantum channels," in *Proceedings 41st Annual Symposium on Foundations of Computer Science*. IEEE, 2000, pp. 547–553.
[68] R. Bhatia, *Matrix analysis*. Springer Science & Business Media, 2013, vol. 169.
[69] T. Kato, *Perturbation theory for linear operators*. Springer Science & Business Media, 2013, vol. 132.
[70] S. Chien, "Augmented ((t,n))-threshold quantum secret sharing schemes," Master's thesis, Princeton University, 2020, senior thesis, available at: http://arks.princeton.edu/ark:/88435/dsp01fb494c46v.
[71] A. Cakan, V. Goyal, C.-D. Liu-Zhang, and J. Ribeiro, "Computational quantum secret sharing," 2023, carnegie Mellon University, NTT Research, NOVA LINCS.
[72] H. Krawczyk, "Secret sharing made short," in *Annual international cryptology conference*. Springer, 1993, pp. 136–146.
[73] A. C. Nascimento, J. Mueller-Quade, and H. Imai, "Improving quantum secret-sharing schemes," *Physical Review A*, vol. 64, no. 4, p. 042311, 2001.
[74] B. Fortescue and G. Gour, "Reducing the quantum communication cost of quantum secret sharing," *IEEE transactions on information theory*, vol. 58, no. 10, pp. 6659–6666, 2012.
[75] R. Cleve, D. Gottesman, and H. Lo, "How to share a quantum secret," *Physical Review Letters*, vol. 83, pp. 648–651, 1999.
[76] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," *Physical review letters*, vol. 83, no. 3, p. 648, 1999.