2024 IEEE 63rd Conference on Decision and Control (CDC)
December 16-19, 2024. MiCo, Milan, Italy

Measuring Quantum Information Leakage Under Detection Threat

Farhad Farokhi and Sejeong Kim

Abstract— **Gentle quantum leakage is proposed as a measure of information leakage to arbitrary eavesdroppers that aim to avoid detection. Gentle (also sometimes referred to as weak or non-demolition) measurements are used to encode the desire of the eavesdropper to evade detection. The gentle quantum leakage meets important axioms proposed for measures of information leakage including positivity, independence, and unitary invariance. Global depolarizing noise, an important family of physical noise in quantum devices, is shown to reduce gentle quantum leakage (and hence can be used as a mechanism to ensure privacy or security). A lower bound for the gentle quantum leakage based on asymmetric approximate cloning is presented. This lower bound relates information leakage to mutual incompatibility of quantum states. A numerical example, based on the encoding in the celebrated BB84 quantum key distribution algorithm, is used to demonstrate the results.**

I. Introduction

Quantum cryptography and key distribution, such as the celebrated BB84 algorithm [1], often rely on two fundamental features of quantum mechanical systems: no cloning theorem and post-measurement state collapse [2]. No cloning theorem states that it is impossible to copy a generic quantum state and therefore an eavesdropper must take direct measurements of the underlying quantum mechanical system that is used for communication (e.g., polarization of photons). Post-measurement state collapse implies that upon observing the quantum mechanical system by the eavesdropper, its state will stochastically and irreparably change, which can be used by the sender or receiver to identify presence of an intruder [1], [3]. Upon detection of the eavesdropper, the authorized users can abandon communication or switch medium to avoid the eavesdropper. This motivates investigating the interplay between information extraction by the eavesdropper (by taking informative measurements) versus its detection by the authorized users (by post-measurement state collapse) to determine the optimal trade-off.

The problem of investigating the trade-off between measurement informativeness and state collapse is not new. It has attracted attention of physicist in the past [4]–[7]. However, they may not be fit for purpose due to two main reasons. First, they assume that the eavesdropper is interested in estimating the entirety of the classical information that is encoded in the quantum system. This restrict our modeling of the eavesdropper. A better approach to investigating eavesdroppers in security and privacy literature is to consider the worst-case information leakage over anything that they try to guess or estimate [8]–[11]. This way, we do not underestimate the eavesdropper and consider a more general threat model. Second, mutual information is not a good measure for information leakage [8]. It was stated in [4] that "mutual information ... may not be the quantities that are most relevant to applications in quantum cryptography." The motivation for mutual information is rooted in data compression and transmission with vanishing error, while an eavesdropper may be content with guessing most likely outcomes, e.g., as an starting point for phishing attacks. Thus even a modest increase in the probability of successfully guessing some attributes of the encoded data can lead to devastating consequences.

In this paper, we develop a notion for information leakage against an arbitrary eavesdropper (one whose intention is not entirely clear to us) that aims to avoid detection. We use gentle measurements, utilized in [12], to encode the desire of the eavesdropper to evade detection. A measurement is called gentle if the post-measurement state remains in proximity of the state prior to measurement with high probability (over outcomes of measurement). The measure of proximity, i.e., the magnitude of the change caused by the measurement, in the gentle measurement framework can be tied to the probability of detection by the Bayesian quantum hypothesis testing [5]. This notion of quantum information leakage, referred to as *gentle quantum leakage*, measures the worst-case multiplicative increase in the probability of correctly guessing any deterministic or randomized function of the private classical data with and without access to the quantum system encoding the-said data. This way, we search over all possible goals for the eavesdropper and do not restrict our analysis.

We derive a semi-explicit formula for the gentle quantum measurement based on the Sibson information of order infinity (an extension of the mutual information [13]). Furthermore, we prove that the gentle quantum leakage meets important axioms for a measure of information leakage including positivity (i.e., gentle quantum leakage is always greater than or equal to zero), independence (i.e., gentle quantum leakage is zero if the quantum state is independent of the classical data), and unitary invariance (gentle quantum leakage remains unchanged by transforming the quantum encoding of the classical data by a unitary channel). These axioms have been formulated for classical and quantum notions of information leakage [8], [9], [11], [14], [15]. We provide upper bounds for the gentle quantum leakage based on the number of the possibilities of the classical data (i.e., the cardinality of its support set) and the dimension of the quantum system used for encoding the data. We prove that global depolarizing noise, an important family of physical noise in quantum devices [16], reduces the gentle quantum leakage and therefore, can be used as a mechanism for

The authors are with the Department of Electrical and Electronic Engineering at the University of Melbourne.
e-mails:{farhad.farokhi, sejeong.kim}@unimelb.edu.au

mitigating security and privacy threats, albeit at the risk of sacrificing utility [17], [18]. We also provide a lower bound for gentle quantum leakage based on asymmetric approximate cloning [19]. A numerical example, based on the encoding in the BB84 [1], is used to demonstrate the results.

The remainder of the paper is organized as follows. Section II presents some preliminary material and notations on quantum systems and information theory. Gentle quantum leakage is presented in Section III. A lower bound based on approximate cloning is presented in Section IV. Numerical results are presented in Section V. Finally, Section VI concludes the paper and presents some directions for future work.

Finally, note that, due to page limitations, most detailed proofs have been removed from the paper after peer-review. The proofs can be found in an online technical report [20].

II. Preliminaries

Finite-dimensional Hilbert spaces are denoted by $\mathcal{H}$. The set of linear operators from $\mathcal{H}_A$ to $\mathcal{H}_B$ is denoted by $\mathcal{L}(\mathcal{H}_A, \mathcal{H}_B)$. When $\mathcal{H}_A = \mathcal{H}_B = \mathcal{H}$, with slight abuse of notation, we write $\mathcal{L}(\mathcal{H})$ instead of $\mathcal{L}(\mathcal{H}_A, \mathcal{H}_B)$. The set of positive semi-definite linear operators on Hilbert space $\mathcal{H}$ is denoted by $\mathcal{P}(\mathcal{H}) \subset \mathcal{L}(\mathcal{H})$. We write $A \geq 0$ when $A \in \mathcal{P}(\mathcal{H})$ and $A \geq B$ if $A - B \geq 0$. Furthermore, the set of positive semi-definite linear operators on Hilbert space $\mathcal{H}$ with unit trace, also known as density operators, is denoted by $\mathcal{S}(\mathcal{H}) \subset \mathcal{P}(\mathcal{H}) \subset \mathcal{L}(\mathcal{H})$. We use lower case Greek letters, such as ρ and σ, to denote density operators. Conventionally, density operators are used to model states of quantum systems [21, § 4]. We define the (normalized) trace distance between any two quantum states $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ as

$$\|\rho - \sigma\|_{\mathrm{tr}} := \frac{1}{2}\,\mathrm{tr}(|\rho - \sigma|),$$

where $|M| = \sqrt{M^\dagger M}$ for any operator $M \in \mathcal{L}(\mathcal{H})$. An important property of the trace distance is that it is unitary invariant, i.e., $\|U(\rho - \sigma)V^\dagger\|_{\mathrm{tr}} = \|\rho - \sigma\|_{\mathrm{tr}}$ for all unitary operators U and V [21, Property 9.1.4]. Note that operator $U \in \mathcal{L}(\mathcal{H})$ is unitary if $U^\dagger U = UU^\dagger = I$. For any two linear operators $A, B \in \mathcal{L}(\mathcal{H})$, $[A, B] = AB - BA$ denotes their commuter. Linear operators $A, B \in \mathcal{L}(\mathcal{H})$ commute if and only if $[A, B] = 0$.

Generalized quantum measurements are modelled using the Positive Operator Valued Measure (POVM) framework. POVMs can model the von Neumann, i.e., projection-based, measurements and their extensions, e.g., when the measurement involves interaction with ancillary systems [22]. A POVM, with the set of possible outcomes $\mathbb{Y}$, is a set of positive semi-definite operators $\mathcal{F} = \{F_y\}_{y\in\mathbb{Y}} \subseteq \mathcal{P}(\mathcal{H})$ such that $\sum_{y\in\mathbb{Y}} F_y = I$. The probability of observing measurement outcome $y \in \mathbb{Y}$ on a quantum system with state $\rho \in \mathcal{S}(\mathcal{H})$ is $\mathrm{tr}(\rho F_y)$. This is commonly called the Born's rule. Note that POVMs do not explicitly consider the post-measurement state of the quantum system, i.e., post-measurement collapse of the state. To also model the post-measurement state collapse, we need to consider an implementation $\mathcal{B} = \{B_y\}_{y\in\mathbb{Y}}$ of POVM $\mathcal{F} = \{F_y\}_{y\in\mathbb{Y}}$ such that $F_y = B_y^\dagger B_y$ for all $y \in \mathbb{Y}$. For any operator B, $B^\dagger$ denotes its complex conjugate transpose. Using implementation $\mathcal{B} = \{B_y\}_{y\in\mathbb{Y}}$, the post-measurement state is given by

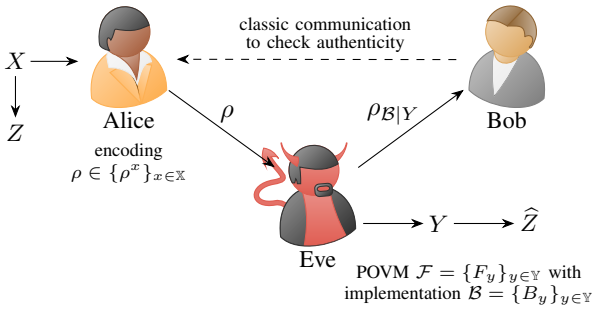

Fig. 1. Communication schematic between Alice, Bob, and Eve.

$$\rho_{\mathcal{B}|y} = \frac{B_y \rho B_y^\dagger}{\mathrm{tr}(B_y \rho B_y^\dagger)} = \frac{B_y \rho B_y^\dagger}{\mathrm{tr}(\rho F_y)},$$

if the outcome $y \in \mathbb{Y}$ is observed and the pre-measurement state is $\rho \in \mathcal{S}(\mathcal{H})$. It is postulated that it is impossible to observe a quantum system, i.e., take measurements, without disturbing its state via the so-called post-measurement state collapse [4]. This is a feature that often underlies quantum cryptography and key distribution [1]. However, some measurements disturb the state more than others. A family of measurements that do not significantly disturb the state are called gentle [12] or weak measurements [4]. We use these measurements to develop a notion of information leakage when the eavesdropper aims to be undetected.

Definition 1 (Gentle Measurements) *Consider the set of states $S \subseteq \mathcal{S}(\mathcal{H})$ and constants $\alpha, \delta \in [0, 1]$.*

The POVM $\mathcal{F} = \{F_y\}_{y\in\mathbb{Y}}$ is (α, δ)-weakly gentle on S if it possesses at least one implementation $\mathcal{B} = \{B_y\}_{y\in\mathbb{Y}}$, i.e., $F_y = B_y^\dagger B_y$ for all $y \in \mathbb{Y}$, such that

$$\mathbb{P}\left\{\|\rho_{\mathcal{B}|Y} - \rho\|_{\mathrm{tr}} \leq \alpha, \forall \rho \in S\right\} \geq 1 - \delta, \tag{1}$$

where the probability is taken with respect to measurement outcomes, i.e., random variable $Y \in \mathbb{Y}$ denotes the measurement outcome. The set of all (α, δ)-weakly gentle POVMs on S is denoted by $\mathcal{G}_{(\alpha,\delta)}(S)$.

The POVM $\mathcal{F} = \{F_y\}_{y\in\mathbb{Y}}$ is (α, δ)-strongly gentle on S if (1) *holds for* all *implementations $\mathcal{B} = \{B_y\}_{y\in\mathbb{Y}}$. The set of all (α, δ)-strongly gentle POVMs on S is denoted by $\overline{\mathcal{G}}_{(\alpha,\delta)}(S)$.*

III. Maximal Leakage with Gentle Measurements

We use discrete random variable $X \in \mathbb{X}$ to model the classical data that must be protected. Without loss of generality, we assume that $p_X(x) = \mathbb{P}\{X = x\} > 0$ for all $x \in \mathbb{X}$; otherwise, we can trim the set $\mathbb{X}$ to only contain elements with non-zero probability. For each $X = x \in \mathbb{X}$, Alice prepares quantum system A in mixed state $\rho^x \in \mathcal{P}(\mathcal{H})$, i.e., encodes x as ρ^x. The ensemble $\mathcal{E} := \{p_X(x), \rho^x\}_{x\in\mathbb{X}}$

models Alice's quantum encoding of the classical data. Alice intends to communicate this quantum system to Bob as in Figure 1. However, this communication maybe intercepted by an eavesdropper, Eve. From the perspective of someone who does not know the realization of classical data X, i.e., Bob and Eve, the state is given by the expected density operator $\rho = \mathbb{E}\{\rho^X\} = \sum_{x\in\mathbb{X}} p_X(x)\rho^x$.

Eve wants to estimate a possibly randomized discrete function of the classical data X, denoted by discrete random variable Z. The nature and composition of this random variable, i.e., the target of the eavesdropping attack, is not known by Alice or Bob. This can only be done by taking measurements of the quantum system, which is modelled by POVM $\mathcal{F} = \{F_y\}_{y\in\mathbb{Y}}$. Let discrete random variable $Y \in \mathbb{Y}$ denote the outcome of the measurement. By Born's rule, $\mathbb{P}\{Y = y \,|\, X = x\} = \mathrm{tr}(\rho^x F_y)$ for all $x \in \mathbb{X}$ and $y \in \mathbb{Y}$. Eve uses the measurement outcome to take a one-shot[1] guess of the random variable Z denoted by the random variable $\widehat{Z}$. Maximal quantum leakage, defined in [9], measures the multiplicative increase of the probability of correctly guessing the realization of any random variable Z with and without access to the measurement outcome Y.

Definition 2 (Maximal Quantum Leakage [9]) *Maximal quantum leakage from random variable X through quantum system A is*

$$\mathcal{Q}(X\to A)_\rho := \sup_{\{F_y\}_{y\in\mathbb{Y}}} \sup_{Z,\widehat{Z}} \log\left(\frac{\mathbb{P}\{Z=\widehat{Z}\}}{\max\limits_{z\in\mathbb{Z}}\mathbb{P}\{Z=z\}}\right) \tag{2a}$$

$$= \sup_{\{F_y\}_{y\in\mathbb{Y}}} \log\left(\sum_{y\in\mathbb{Y}} \max_{x\in\mathbb{X}} \mathrm{tr}(\rho^x F_y)\right), \tag{2b}$$

where, in (2a)*, the inner supremum is taken over all random variables $Z, \widehat{Z} \in \mathbb{Z}$ with arbitrary finite support set $\mathbb{Z}$ and the outer supremum is taken over all POVMs $\mathcal{F} = \{F_y\}_{y\in\mathbb{Y}}$ with arbitrary finite outcome set $\mathbb{Y}$.*

For maximal quantum leakage, defined above, we search over all measurements to find one that results in the most information gain, measured by multiplicative increase in the probability of correctly guessing a secret. This would imply that the post-measurement state could be arbitrarily disturbed. This disturbance can be used by Alice or Bob to identify presence of an eavesdropper (in which case they can cease communication or switch to a different medium). For instance, the famous quantum key distribution algorithm of BB84 [1] uses the post-measurement state disturbance, no-cloning theorem in quantum systems, and access to a classical communication channel to identify presence of an eavesdropper. Therefore, it is postulated that Eve must use gentle or weak measurements to avoid getting caught [4]. Note that the use of the trace-distance in the definition of gentle measurements can be justified if the Alice or Bob use the Bayesian hypothesis-testing to identify presence of an eavesdropper [5]. Other definitions, e.g., using fidelity [4], [5], can be also used. However, they can be translated into the definition relying on trace distance due to the relationship between fidelity and trace distance [21, Theorem 9.3.1].

[1]Number of guesses is immaterial in measuring information leakage [9].

Definition 3 (Gentle Quantum Leakage) *For any $\alpha, \delta \in [0,1]$, (α,δ)-*weakly *gentle quantum leakage from random variable X through quantum system A is*

$$\mathcal{L}_{(\alpha,\delta)}(X\to A)_\rho := \sup_{\{F_y\}_y\in\mathcal{G}_{(\alpha,\delta)}(S)} \sup_{Z,\widehat{Z}} \log_2\left(\frac{\mathbb{P}\{Z=\widehat{Z}\}}{\max\limits_{z\in\mathbb{Z}}\mathbb{P}\{Z=z\}}\right), \tag{3}$$

*where the outer supremum is now taken over the set of all (α,δ)-*weakly *gentle measurements on $S := \{\rho^x\}_{x\in\mathbb{X}}$ denoted by $\mathcal{G}_{(\alpha,\delta)}(S)$. Similarly, (α,δ)-*strongly *gentle quantum leakage is*

$$\overline{\mathcal{L}}_{(\alpha,\delta)}(X\to A)_\rho := \sup_{\{F_y\}_y\in\overline{\mathcal{G}}_{(\alpha,\delta)}(S)} \sup_{Z,\widehat{Z}} \log_2\left(\frac{\mathbb{P}\{Z=\widehat{Z}\}}{\max\limits_{z\in\mathbb{Z}}\mathbb{P}\{Z=z\}}\right), \tag{4}$$

*where the outer supremum is now taken over the set of all (α,δ)-*strongly *gentle measurements.*

This notion of information leakage keeps the disturbance on the state caused by measurement below α with probability of at least $1-\delta$ (with respect to measurement outcomes). This way, we can investigate the trade-off between information leakage and Eve's chance of getting caught by Alice or Bob.

Corollary 1: The following properties hold:

- $\mathcal{L}_{(\alpha,\delta)}(X\to A)_\rho$ and $\overline{\mathcal{L}}_{(\alpha,\delta)}(X\to A)_\rho$ are non-decreasing in $\alpha,\delta\in[0,1]$;
- $\mathcal{L}_{(\alpha,\delta)}(X\to A)_\rho \geq \overline{\mathcal{L}}_{(\alpha,\delta)}(X\to A)_\rho$ for all $\alpha,\delta\in[0,1]$;
- $\mathcal{L}_{1,\delta}(X\to A)_\rho = \mathcal{L}_{\alpha,1}(X\to A)_\rho = \overline{\mathcal{L}}_{1,\delta}(X\to A)_\rho = \overline{\mathcal{L}}_{\alpha,1}(X\to A)_\rho = \mathcal{Q}(X\to A)_\rho$ for all $\alpha,\delta\in[0,1]$.

Proof: These properties can be immediately seen from that $\overline{\mathcal{G}}_{(\alpha,\delta)}(\{\rho^x\}_{x\in\mathbb{X}}) \subseteq \mathcal{G}_{(\alpha,\delta)}(\{\rho^x\}_{x\in\mathbb{X}})$, and that $\mathcal{G}_{(\alpha,\delta)}(\{\rho^x\}_{x\in\mathbb{X}}) \subseteq \mathcal{G}_{(\alpha',\delta')}(\{\rho^x\}_{x\in\mathbb{X}})$ and $\overline{\mathcal{G}}_{(\alpha,\delta)}(\{\rho^x\}_{x\in\mathbb{X}}) \subseteq \overline{\mathcal{G}}_{(\alpha',\delta')}(\{\rho^x\}_{x\in\mathbb{X}})$ if $\alpha'\geq\alpha$ and $\delta'\geq\delta$. Also, as $\alpha\to 1$ or $\delta\to 1$, $\mathcal{G}_{(\alpha,\delta)}(\{\rho^x\}_{x\in\mathbb{X}})$ and $\overline{\mathcal{G}}_{(\alpha,\delta)}(\{\rho^x\}_{x\in\mathbb{X}})$ converges to the set of all POVMs. ■

Using the same line of reasoning as in the maximal quantum leakage in [9], we can derive a semi-explicit formula for the gentle quantum leakage. This derivation follows from eliminating the first supremum on random variables Z and $\widehat{Z}$ using their classical counterpart, i.e., maximal leakage, in [8]. The following result reformulates the gentle quantum leakage using the Sibson mutual information of order infinity, which is a generalized notion of information in classical information theory and can be reviewed in [8], [13].

Corollary 2: The gentle quantum leakage is

$$\mathcal{L}_{(\alpha,\delta)}(X\to A)_\rho = \sup_{\{F_y\}_y\in\mathcal{G}_{(\alpha,\delta)}(\{\rho^x\}_{x\in\mathbb{X}})} I_\infty(X;Y), \tag{5}$$

$$\overline{\mathcal{L}}_{(\alpha,\delta)}(X\to A)_\rho = \sup_{\{F_y\}_y\in\overline{\mathcal{G}}_{(\alpha,\delta)}(\{\rho^x\}_{x\in\mathbb{X}})} I_\infty(X;Y), \tag{6}$$

where $I_\infty(X;Y)$ is the Sibson mutual information of order infinity between random variables X and Y computed as

$$I_\infty(X;Y) := \log_2\left(\sum_{y\in\mathbb{Y}} \max_{x\in\mathbb{X}:p_X(x)>0} \mathbb{P}\{Y=y\,|\,X=x\}\right) = \log_2\left(\sum_{y\in\mathbb{Y}} \max_{x\in\mathbb{X}} \operatorname{tr}(\rho^x F_y)\right).$$

Proof: The proof follows from applying Theorem 1 in [8] to resolve the supremum on Z and $\widehat{Z}$. ∎

In what follows, we prove that the gentle quantum leakage is an appropriate notion of information leakage by demonstrating that it meets important axioms [8], [9], [11], [14], [15], such as positivity (i.e., gentle quantum leakage is always greater than or equal to zero), independence (i.e., gentle quantum leakage is zero if the quantum state is independent of the classical data), and unitary invariance (gentle quantum leakage remains unchanged by transforming the quantum encoding of the classical data by a unitary channel).

Proposition 1 (Positivity and Independence) *The following properties hold:*

- $\mathcal{L}_{(\alpha,\delta)}(X\to A)_\rho \geq 0$ *with equality if and only if* $\rho^x = \rho^{x'}$ *for all* $x, x' \in \mathbb{X}$*;*
- $\overline{\mathcal{L}}_{(\alpha,\delta)}(X\to A)_\rho \geq 0$ *with equality if* $\rho^x = \rho^{x'}$ *for all* $x, x' \in \mathbb{X}$.

Proof: See [20]. ∎

In the next result, we show that the strongly gentle quantum leakage remains unchanged by application of unitary quantum channels on the quantum encoding of the classical data. Unitary operators are often used for quantum computing [2] and quantum machine learning [23]. Therefore, this result demonstrates that quantum information leakage, measured by strongly gentle quantum leakage, cannot increase by employing arbitrary quantum computing routines (which also contains classical computing routines as a subset).

Proposition 2 (Unitary Invariance) *For any unitary channel* $\mathcal{U}(\rho) = U\rho U^\dagger$ *with unitary operator* $U \in \mathcal{L}(\mathcal{H})$,

$$\overline{\mathcal{L}}_{(\alpha,\delta)}(X\to A)_{\mathcal{U}(\rho)} = \overline{\mathcal{L}}_{(\alpha,\delta)}(X\to A)_\rho.$$

Proof: See [20]. ∎

For the weakly gentle quantum leakage, we may not be able to achieve unitary invariance. Instead, we prove a weak data-processing inequality that shows that the weakly gentle quantum leakage under application of the unitary operator can be bounded. This is done in the following proposition.

Proposition 3 (Weak Data-Processing Inequality) *For any unitary channel* $\mathcal{U}(\rho) = U\rho U^\dagger$ *with unitary operator* $U \in \mathcal{L}(\mathcal{H})$,

$$\mathcal{L}_{(\alpha,\delta)}(X\to A)_{\mathcal{U}(\rho)} \leq \mathcal{L}_{(\alpha+\beta(\mathcal{U}),\delta)}(X\to A)_\rho,$$

where $\beta(\mathcal{U}) := \sup_{\rho\in\{\rho^x\}_{x\in\mathbb{X}}} \|\mathcal{U}(\rho)-\rho\|_{\mathrm{tr}}$.

Proof: See [20]. ∎

In the next proposition, we derive an upper bound for the gentle quantum leakage based on maximal quantum leakage. This demonstrates that, as expected, a discrete random variable $X \in \mathbb{X}$ has no more than $\log_2(|\mathbb{X}|)$ bits of information for an adversary to learn. In addition, the amount of leaked information is upper bounded by $2\log_2(\dim(\mathcal{H}))$. Hence, embedding or encoding classical information in a "small" quantum system, i.e., $\dim(\mathcal{H}) \ll |\mathbb{X}|$, can restrict the leakage (and perhaps simultaneously the utility of such encoding for information processing).

Proposition 4 (Upper Bound) $\overline{\mathcal{L}}_{(\alpha,\delta)}(X\to A)_{\mathcal{U}(\rho)} \leq \mathcal{L}_{(\alpha,\delta)}(X\to A)_{\mathcal{U}(\rho)} \leq \min\{\log_2(|\mathbb{X}|), 2\log_2(\dim(\mathcal{H}))\}$ *if* $\rho \in \mathcal{S}(\mathcal{H})$.

Proof: The proof follows from Corollary 1 and the upper bound for maximal quantum leakage in [9]. ∎

In the next proposition, we show that the gentle quantum leakage is reduced by application of a global depolarizing channel $\mathcal{D}_p : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{H})$ defined as

$$\mathcal{D}_p(\rho) := \frac{p}{\dim(\mathcal{H})} I + (1-p)\rho, \tag{7}$$

where $p \in [0,1]$ is a probability parameter capturing the magnitude of the depolarization "noise". This implies that gentle quantum leakage accords with intuition (that quantum noise can reduce the information leakage) and follows similar results on privacy in quantum systems [9], [24].

Proposition 5: For global depolarizing channel $\mathcal{D}_p$,

$$\mathcal{L}_{(\alpha,\delta)}(X\to A)_{\mathcal{D}_p(\rho)} = \log_2(p+(1-p)2^{\mathcal{L}_{(\alpha,\delta)}(X\to A)_\rho}),$$
$$\overline{\mathcal{L}}_{(\alpha,\delta)}(X\to A)_{\mathcal{D}_p(\rho)} = \log_2(p+(1-p)2^{\overline{\mathcal{L}}_{(\alpha,\delta)}(X\to A)_\rho}).$$

Particularly,

$$\frac{\mathrm{d}}{\mathrm{d}p}\mathcal{L}_{(\alpha,\delta)}(X\to A)_{\mathcal{D}_p(\rho)} < 0 \text{ if } \mathcal{L}_{(\alpha,\delta)}(X\to A)_\rho > 0,$$
$$\frac{\mathrm{d}}{\mathrm{d}p}\overline{\mathcal{L}}_{(\alpha,\delta)}(X\to A)_{\mathcal{D}_p(\rho)} < 0 \text{ if } \overline{\mathcal{L}}_{(\alpha,\delta)}(X\to A)_\rho > 0,$$

which shows that gentle quantum leakage is decreasing in probability parameter p.

Proof: Following [9], we know that

$$\sum_{y\in\mathbb{Y}} \max_{x\in\mathbb{X}} \operatorname{tr}(\mathcal{D}_p(\rho^x)F_y) = p + (1-p)\sum_{y\in\mathbb{Y}} \max_{x\in\mathbb{X}} \operatorname{tr}(\rho^x F_y).$$

Therefore,

$$\begin{aligned}
&\mathcal{L}_{(\alpha,\delta)}(X\to A)_{\mathcal{D}_p(\rho)} \\
&\quad= \log_2\left(\sup_{\{F_y\}_y} \sum_{y\in\mathbb{Y}} \max_{x\in\mathbb{X}} \operatorname{tr}(\mathcal{D}_p(\rho^x)F_y)\right) \\
&\quad= \log_2\left(p+(1-p)\sup_{\{F_y\}_y} \sum_{y\in\mathbb{Y}} \max_{x\in\mathbb{X}} \operatorname{tr}(\rho^x F_y)\right) \\
&\quad= \log_2(p+(1-p)2^{\mathcal{L}_{(\alpha,\delta)}(X\to A)_\rho}),
\end{aligned}$$

where the supremum is taken over $\mathcal{G}_{(\alpha,\delta)}(\{\rho^x\}_{x\in\mathbb{X}})$. The proof for $\overline{\mathcal{L}}_{(\alpha,\delta)}(X\to A)_{\mathcal{D}_p(\rho)}$ follows from taking the supremum over $\overline{\mathcal{G}}_{(\alpha,\delta)}(\{\rho^x\}_{x\in\mathbb{X}})$. ∎

IV. Approximate Cloning

A quantum cloner is a quantum channel $T : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{H}) \times \mathcal{S}(\mathcal{H})$. This is often referred to as $1 \to 2$ quantum cloning because 2 copies from 1 state are created. Ideally, we would like this mapping to be such that $T(\rho) = \rho \otimes \rho$ for any $\rho \in \mathcal{S}(\mathcal{H})$. This is however forbidden by the rules of quantum system (particularly linearity of quantum channels) [25]. Despite this negative result, imperfect or approximate cloning has been shown to be achievable [26], [27]. Let T_i denote the quantum channel to the i-th copy of quantum state, i.e., $T_i(\rho) = \mathrm{tr}_{-i}(T(\rho))$, where tr_{-i} denotes the partial trace with respect all quantum systems except the i-th one.

Theorem 1 (Cloning Region [28]) *For all $p_1, p_2 \in [0,1]$, there exists quantum cloner T such that $T_i = \mathcal{D}_{p_i}$ if and only if*

$$\frac{d}{2}(d(2-p_1-p_2)+\sqrt{d^2(p_1-p_2)^2-4(1-p_1)(1-p_2)}) - (2-p_1-p_2) \leq (d^2-1),$$

where $d := \dim(\mathcal{H})$.

We can use this description of the achievable approximate cloning to provide a lower bound for the weakly gentle quantum leakage. This is explored in the next proposition.

Proposition 6: For all $\alpha, \delta \in [0,1]$, the weakly gentle quantum leakage is lower bounded by

$$\mathcal{L}_{(\alpha,\delta)}(X \to A)_\rho \geq \mathcal{L}_{(\alpha,0)}(X \to A)_\rho \geq \underline{\mathcal{L}}_\alpha(\{\rho^x\}_{x\in\mathbb{X}}),$$

where $\underline{\mathcal{L}}_\alpha(\{\rho^x\}_{x\in\mathbb{X}}) := \log_2(p_2^* + (1-p_2^*)2^{\mathcal{Q}(X\to A)_\rho})$ and $d = \dim(\mathcal{H})$ with

$$\begin{aligned}(p_1^*, p_2^*) \in \min_{(p_1,p_2)} \quad & p_2, \\ \text{s.t.} \quad & 0 \leq p_1 \leq 1, \\ & 0 \leq p_2 \leq 1, \\ & p_1 \leq \frac{\alpha}{\|I/\dim(\mathcal{H}) - \rho^x\|_{\mathrm{tr}}}, \forall x \in \mathbb{X}, \\ & \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}^\top \begin{bmatrix} 2d^2 - 1 - \frac{d^4}{4} & 1 - \frac{d^4}{4} \\ 1 - \frac{d^4}{4} & 2d^2 - 1 - \frac{d^4}{4} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \end{bmatrix} \\ & \quad + \begin{bmatrix} -2-d^2 & -2-d^2 \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \end{bmatrix} + 3 \leq 0.\end{aligned}$$

Proof: The second copy can be used to extract secret information by Eve. By using the cloning technique provided in Theorem 1, we can see that the second cloned state contains $\log_2(p_2+(1-p_2)2^{\mathcal{Q}(X\to A)_\rho})$ bits of information [9]. Furthermore, the first copy can be passed to Bob for which the disturbance is given by $\|T_1(\rho)-\rho\|_{\mathrm{tr}} = p_1\|I/\dim(\mathcal{H})-\rho\|_{\mathrm{tr}}$. Finally, the last constraint follows from the condition in Theorem 1. ∎

Remark 1 (Convexity) *The optimization problem in Proposition 6 is convex for $\dim(\mathcal{H}) = 2$. Therefore, for a qubit, i.e., when $\dim(\mathcal{H}) = 2$, the lower bound can be easily computed. Unfortunately, the last constraint becomes non-convex if $\dim(\mathcal{H}) > 2$.*

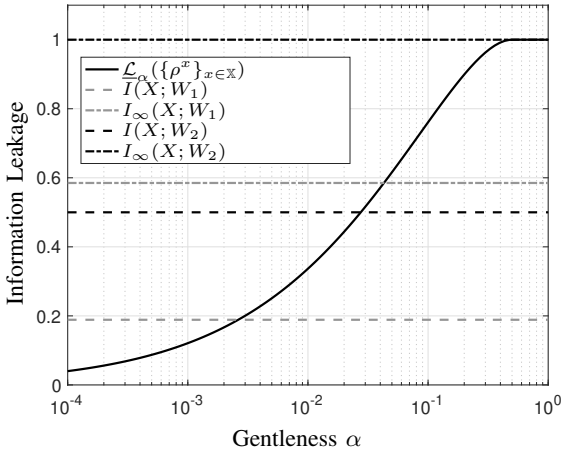

Fig. 2. Information leakage and its lower bound versus weakly gentle measurement parameter α.

Remark 2 (Incompatibility) *A similar measure to $\underline{\mathcal{L}}_\alpha(\{\rho^x\}_{x\in\mathbb{X}})$ in Proposition 6 has been proposed as a measure of mutual incompatibility of states within $\{\rho^x\}_{x\in\mathbb{X}}$, albeit for pure states and based on symmetric approximate cloning [19]. Here, $\underline{\mathcal{L}}_\alpha(\{\rho^x\}_{x\in\mathbb{X}})$ generalizes this notion of mutual incompatibility to asymmetric approximate cloning and potentially mixed states. It should be noted that if $\{\rho^x\}_{x\in\mathbb{X}}$ are mutually compatible, i.e., if ρ^x and $\rho^{x'}$ commute for all $x, x' \in \mathbb{X}$, perfect cloning is possible and thus we can attain maximal information leakage with no state disturbance.*

Corollary 3: For all $\alpha, \delta \in [0,1]$, $\mathcal{L}_{(\alpha,\delta)}(X \to A)_\rho = \mathcal{L}_{(\alpha,0)}(X \to A)_\rho = \mathcal{Q}(X \to A)_\rho$ if $[\rho^x, \rho^{x'}] = 0$ for all $x, x' \in \mathbb{X}$.

V. Numerical Example

Consider the BB84 scheme in [1]. This is a scheme for quantum key distribution and its security relies on non-cloning theorem and post-measurement state collapse. Consider uniformly distributed random variable $X = (X_1, X_2) \in \{0,1\}^2$. The sender, i.e., Alice in Figure 1, encodes the random variable X into a two-dimensional quantum system, i.e., a qubit, according to

$$\rho^x = \begin{cases} |0\rangle\langle 0|, & x = (0,0), \\ |1\rangle\langle 1|, & x = (0,1), \\ |+\rangle\langle +|, & x = (1,0), \\ |-\rangle\langle -|, & x = (1,1), \end{cases}$$

where $\{|0\rangle, |1\rangle\}$ is the computational basis or the Z-basis, and $\{|+\rangle, |-\rangle\}$ is the X-basis. Here, X and Z refer to Pauli matrices [2]. The qubit, for instance, can model the photon polarization when establishing quantum communication using single photons. Given that it is not possible to clone an arbitrary quantum state, the eavesdropper must measure the state directly or via an ancillary system interacting with it (e.g., based on approximate cloning). For instance, the eavesdropper can toss a coin and, based on the outcome, measure the state either in the Z-basis or the X-basis. This

measurement is denoted by W_1 in what follows. Another approach is to always measure in the X-basis. This measurement is denoted by W_2 in what follows. Both these measurement strategies result in a non-trivial change of the state (as they are projection based), which the sender or the receiver can use to identify the presence of a malicious party and thus abandon communication (i.e., key sharing protocol) with high probability. This was used to establish the safety of the BB84 algorithm. Instead of the proposed measurement strategies, the eavesdropper can use gentle measurements proposed in this paper to extract some information, albeit not the maximum possible amount, while reducing the detection probability. Note that as α and δ (i.e., the gentleness) vary the amount of extracted information changes but also the probability of detection by the sender or receiver.

Figure 2 illustrates information leakage versus weakly gentle measurement parameter α. The solid curve illustrates the lower bound $\underline{\mathcal{L}}_\alpha(\{\rho^x\}_{x\in\mathbb{X}})$ in Proposition 6. Other measures of information leakage that do not rely on gentle measurement are also demonstrated for comparison. The maximum amount of information that can be extracted, captured by the maximal quantum leakage $\mathcal{Q}(X \to A)_\rho$ and attained by measurement W_2, is 1 bit. As we increase $\alpha \to 1$, the lower bound gets closer to the maximal quantum leakage. As we reduce $\alpha \to 0$, the lower bound reduces. It is interesting to that for a relatively small $\alpha = 0.1$ (which reduces the chance of Eve getting caught significantly), the eavesdropper can still steal a significant amount of information $\mathcal{L}_{(0.1,\delta)}(X \to A)_\rho \geq \underline{\mathcal{L}}_{0.1}(\{\rho^x\}_{x\in\mathbb{X}}) = 0.7608$ for any $\delta \in [0, 1]$.

VI. Conclusions and Future Work

We developed and studied a new notion for quantum information leakage against arbitrary eavesdroppers that aim to avoid detection. Gentle measurements were used to encode the desire of the adversary to evade detection. Future work can focus on proving data-processing inequality for general quantum channels and (sub-)additivity when accessing multiple quantum systems. Also, a numerical algorithm for computing the gentle quantum leakage can be developed.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, 2014.

[2] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[3] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, "Eavesdropping on quantum-cryptographical systems," *Physical Review A*, vol. 50, no. 2, p. 1047, 1994.

[4] C. A. Fuchs and A. Peres, "Quantum-state disturbance versus information gain: Uncertainty relations for quantum information," *Phys. Rev. A*, vol. 53, no. 4, p. 2038, 1996.

[5] C. A. Fuchs, "Information gain vs. state disturbance in quantum theory," *Fortschritte der Physik: Progress of Physics*, vol. 46, no. 4-5, pp. 535–565, 1998.

[6] C. A. Fuchs and K. Jacobs, "Information-tradeoff relations for finite-strength quantum measurements," *Physical Review A*, vol. 63, no. 6, p. 062305, 2001.

[7] K. Banaszek, "Information gain versus state disturbance for a single qubit," *Open Systems & Information Dynamics*, vol. 13, no. 1, pp. 1–16, 2006.

[8] I. Issa, A. B. Wagner, and S. Kamath, "An operational approach to information leakage," *IEEE Transactions on Information Theory*, vol. 66, no. 3, pp. 1625–1657, 2019.

[9] F. Farokhi, "Maximal information leakage from quantum encoding of classical data," *Phys. Rev. A*, vol. 109, p. 022608, Feb 2024.

[10] J. Liao, O. Kosut, L. Sankar, and F. du Pin Calmon, "Tunable measures for information leakage and applications to privacy-utility tradeoffs," *IEEE Transactions on Information Theory*, vol. 65, no. 12, pp. 8043–8066, 2019.

[11] F. Farokhi and N. Ding, "Measuring information leakage in non-stochastic brute-force guessing," in *2020 IEEE Information Theory Workshop (ITW)*, pp. 1–5, IEEE, 2021.

[12] S. Aaronson and G. N. Rothblum, "Gentle measurement of quantum states and differential privacy," in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pp. 322–333, 2019.

[13] S. Verdu, "α-mutual information," in *2015 Information Theory and Applications Workshop (ITA)*, pp. 1–6, 2015.

[14] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, "On quantum Rényi entropies: A new generalization and some properties," *Journal of Mathematical Physics*, vol. 54, no. 12, 2013.

[15] K. M. R. Audenaert and N. Datta, "α-z-Rényi relative entropies," *Journal of Mathematical Physics*, vol. 56, no. 2, p. 022202, 2015.

[16] J. Vovrosh, K. E. Khosla, S. Greenaway, C. Self, M. S. Kim, and J. Knolle, "Simple mitigation of global depolarizing errors in quantum simulations," *Phys. Rev. E*, vol. 104, p. 035309, Sep 2021.

[17] F. Farokhi, "Barycentric and pairwise rényi quantum leakage," *arXiv preprint arXiv:2402.06156*, 2024.

[18] T. Nuradha, Z. Goldfeld, and M. M. Wilde, "Quantum pufferfish privacy: A flexible privacy framework for quantum systems," *arXiv preprint arXiv:2306.13054*, 2023.

[19] A. Mitra and P. Mandayam, "On optimal cloning and incompatibility," *Journal of Physics A: Mathematical and Theoretical*, vol. 54, no. 40, p. 405303, 2021.

[20] F. Farokhi and S. Kim, "Measuring quantum information leakage under detection threat," 2024. Technical Note, arXiv preprint arXiv:2403.11433, `https://arxiv.org/abs/2403.11433`.

[21] M. Wilde, *Quantum Information Theory*. Quantum Information Theory, Cambridge University Press, 2013.

[22] H. Wiseman and G. Milburn, *Quantum Measurement and Control*. Cambridge University Press, 2010.

[23] M. Benedetti, E. Lloyd, S. Sack, and M. Fiorentini, "Parameterized quantum circuits as machine learning models," *Quantum Science and Technology*, vol. 4, no. 4, p. 043001, 2019.

[24] C. Hirche, C. Rouzé, and D. S. Franca, "Quantum differential privacy: An information theory perspective," *IEEE Transactions on Information Theory*, vol. 69, no. 9, pp. 5771–5787, 2023.

[25] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[26] D. Bruß, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin, "Optimal universal and state-dependent quantum cloning," *Physical Review A*, vol. 57, no. 4, p. 2368, 1998.

[27] V. Bužek and M. Hillery, "Quantum copying: Beyond the no-cloning theorem," *Physical Review A*, vol. 54, no. 3, p. 1844, 1996.

[28] I. Nechita, C. Pellegrini, and D. Rochette, "The asymmetric quantum cloning region," *Letters in Mathematical Physics*, vol. 113, no. 3, p. 74, 2023.

Appendix I
Useful Lemma

Lemma 1: Consider

$$B_+ = \sqrt{\frac{1-2\epsilon^2}{2}} I + \epsilon M,$$
$$B_- = \sqrt{\frac{1-2\epsilon^2}{2}} I - \epsilon M,$$
$$B_0 = \sqrt{2}\epsilon (I - M^2)^{1/2},$$

for semi-positive definite operator M. Then $\{F_+, F_-, F_0\}$ with $F_y = B_y B_y^\dagger$ with $y \in \{+, -, 0\}$ forms a POVM. For any $\alpha > 0$, there exists $\epsilon' > 0$ such that, for all $0 \leq \epsilon \leq \epsilon'$, $\{F_+, F_-, F_0\}$ is (α, δ)-weakly gentle on any $S \subseteq \mathcal{S}(\mathcal{H})$.

Proof: See [20]. ∎