TQC TALKS

@IIIT-DELHI

Meeting Link
March 1, 8PM IST

ARMANDO ANGRISANI

A unifying framework for differentially private quantum algorithms

(Joint work with Mina Doosti and Elham Kashefi)

ABSTRACT

Differential privacy is a widely used notion of security that enables the processing of sensitive information. In short, differentially private algorithms map "neighbouring" inputs to close output distributions. Prior work proposed several quantum extensions of differential privacy, each of them built on substantially different notions of neighbouring quantum states.

In this paper, we propose a novel and general definition of neighbouring quantum states. We demonstrate that this definition captures the underlying structure of quantum encodings and can be used to provide exponentially tighter privacy guarantees for quantum measurements.

Our approach combines the addition of classical and quantum noise and is motivated by the noisy nature of near-term quantum devices. Moreover, we also investigate an alternative setting where we are provided with multiple copies of the input state. In this case, differential privacy can be ensured with little loss in accuracy combining concentration of measure and noise-adding mechanisms.

Finally, we complement our theoretical findings with an empirical estimation of the certified adversarial robustness ensured by differentially private measurements.

BIOGRAPHY

Armando is a postdoctoral researcher working at EPFL in Zoe Holmes's group. His research interests span quantum learning theory, variational quantum algorithms and privacy.

Prior to joining EPFL, Armando completed his doctorate at Sorbonne University and his undergraduate studies at Sapienza University. His doctoral thesis explores the disparate impact of noise in quantum computation through the lens of quantum statistical queries, differential privacy and exponential concentration in variational quantum algorithms.

Website: https://sites.google.com/view/angrisani

meet.google.com/hkk-tias-vbe

Friday, 1st March, 8:00 PM IST

arxiv.org/abs/2307.04733

https://braqiiit.github.io/Talks.html