

Optimal depth and a novel approach to variational quantum process tomography

Vladlen Galetsky*, Pol Julià Farré†, Soham Ghosh*, Christian Deppe† and Roberto Ferrara*

*Technical University of Munich

†Technical University of Braunschweig

Email: vladlen.galetsky@tum.de, pol.julia-farre@tu-braunschweig.de, soham.ghosh@tum.de, christian.deppe@tu-braunschweig.de, roberto.ferrara@tum.de

Abstract—In this work, we present two new methods for Variational Quantum Circuit (VQC) Process Tomography onto n qubits systems: PT_VQC and U-VQSVD.

Compared to the state of the art, PT_VQC halves in each run the required amount of qubits for process tomography and decreases the required state initializations from 4^n to just 2^n , all while ensuring high-fidelity reconstruction of the targeted unitary channel U . It is worth noting that, for a fixed reconstruction accuracy, PT_VQC achieves faster convergence per iteration step compared to Quantum Deep Neural Network (QDNN) and tensor network schemes.

The novel U-VQSVD algorithm utilizes variational singular value decomposition to extract eigenvectors (up to a global phase) and their associated eigenvalues from an unknown unitary representing a general channel. We assess the performance of U-VQSVD by executing an attack on a non-unitary channel Quantum Physical Unclonable Function (QPUF). U-VQSVD outperforms an uninformed impersonation attack (using randomly generated input states) by a factor of 2 to 5, depending on the qubit dimension.

For the two presented methods, we propose a new approach to calculate the complexity of the displayed VQC, based on what we denote as optimal depth.

Index Terms—VQC, Process tomography, Optimal depth, Quantum Computation, Singular Value Decomposition.

I. INTRODUCTION

A. Process tomography

Quantum tomography plays an essential role in the security assessment and characterization of channel and state evolution in Noisy Intermediate Scale Quantum (NISQ) devices [1], [2]. A class of promising candidates, ranging from Quantum Deep Neural Networks (QDNN) [3], tensor networks [4], Variational Quantum Circuit (VQC) [5], [6] and quantum compilation algorithms [7], try to perform state and process tomography beyond the current classical computation capabilities.

In process tomography, certain approaches presume particular symmetries within the target circuit. For instance, tensor networks [4] rely on the notion of low entanglement structures. In unsupervised learning and QDNN, algorithms extract multidimensional probability distributions from raw data. The considerable expressivity of such models enables the retention of assumptions regarding high entanglement degrees in the unitary under study [8].

As the system to be queried scales, state and unitary reconstruction become resource-intensive tasks, often resulting in

an exponential overhead [9]. The poor scalability, the lengthy circuit depths and the extensive number of initializations and iterations required to minimize the objective function render VQC schemes unreliable for NISQ device applications. To mitigate these challenges, we propose in Section III-C a new VQC process tomography scheme called PT_VQC.

B. Process tomography of unitary evolutions

Studying non-unitary channels presents a more intricate task. One proposed solution introduces convex optimization [10] to address this challenge. However, this approach relies on understanding the constraints of the process matrix and assumes the structure of the channel under examination. Another proposed method utilizes classical shadows [11], which are based on shadow tomography techniques. However, the classical shadow post-processing becomes highly inefficient as the amount of qubits n scales up. Additionally, for Clifford shadows, prior knowledge of the subsystem is required to perform the non-unitary reconstruction.

We instead introduce a novel solution in Section III-E: the U-VQSVD scheme. We showcase its effectiveness by executing an impersonation attack against a non-unitary Quantum Physical Unclonable Function (QPUF) channel, reconstructing the singular values and vectors of the unknown unitary evolution defining it.

C. Quantum Physical Unclonable Function (QPUF)

QPUFs are hardware-based unclonable devices with an inherent randomness [12], [13], [14] that can be produced, for example, by having an imperfection within an optical crystal. Based on a set of challenges, such randomness results into a production of a unique and unpredictable set of responses and this randomized mapping can be harnessed within the realm of secure authentication.

Recent research [12] introduced a mathematical framework that, for the first time, provided a QPUF scheme with provable security against quantum adversaries, referred to as "Quantum selective unforgeability". However, according to [12] and [15], the security notion they define under the label "Quantum existential unforgeability" is still nonexistent in a unitary QPUF. Subsequently, [16] established an analogous notion of existential unforgeability for their designed non-unitary channel-based QPUF.

We numerically show that U-VQSVD does not break the security notions of [16], while still performing better than an attacker employing random states during authentication.

II. OUR CONTRIBUTIONS

We divide our set of contributions into two main parts. The former arises from a new process tomography algorithm called PT_VQC, found in Section. III-C. In contrast, the approach proposed in [5] relies on an inefficient SWAP-test algorithm to define their cost function, necessitating 4^n state initializations for a complete reconstruction of the target unitary. Such high requirements for VQC process tomography schemes render them slow and unreliable for NISQ device applications, particularly those reliant on qubit dimensionality.

We instead deliver an enhanced scheme by introducing an alternative quantum circuit architecture and redefining the cost function. Notably, we reduce the required state initializations from 4^n to just 2^n and halve for each run the required number of qubits. As a consequence, we improve the processing time of the algorithm while, in parallel, enhancing the accuracy of its gradient computation by applying the 4-term shift rule. We conducted a comparative analysis of the efficiency and cost of the PT_VQC algorithm against variational Matrix Product Operators (MPO) based on tensor networks [4], as well as against QDNN [3].

For the second main contribution, we introduce a new algorithm called U-VQSVD, found in Section. III-E. U-VQSVD is inspired by the variational quantum singular value decomposition scheme proposed in [17]. Our novel proposal allows us to learn unknown general channels by efficiently reconstructing their eigenvalues and eigenvectors up to a phase. Furthermore, we evaluate the effectiveness of our new process tomography scheme by constructing an impersonation attack on the authentication protocol of a Phase Estimation-based QPUF (PE-QPUF) [16]. This assessment involves comparing the capabilities of an attacker employing random states to those of an attacker utilizing U-VQSVD to generate input states, alongside a trusted party.

Finally, we discuss how to select the depth of the VQC introducing the concept of optimal depth and providing the reader with a guideline for its estimation.

III. METHODS

A. Notation

We denote vectors as, e.g., $\hat{\theta}$. $\hat{\theta}_j$ represents the j_{th} block of $\hat{\theta}$, while θ_j denotes the j_{th} parameter of $\hat{\theta}$. Quantum gates are defined with upper case letters, e.g., $RY(\theta)$. U is the targeted unitary and U_{VQC} is the unitary representing the variational quantum circuit. A chain of quantum gates is denoted via a hyphen connecting two gates, e.g., $RY(\theta_0)$ - $RX(\theta_1)$. For pure quantum states, we use the Dirac bra-ket notation $|\psi\rangle$ and lowercase Greek letters, e.g., ρ and σ , for general density-matrix states. The variables t and a represent the number of target and ancilla qubits of the QPUF, respectively. We denote the chosen depth of the VQC as d .

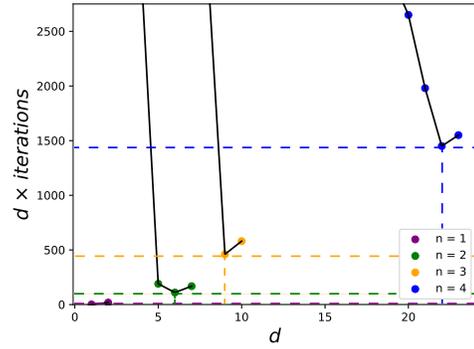


Fig. 1. Amount of required resources, as a function of the depth, characterized by the depth times the maximum number of iterations needed to learn 10 different sets of eigenvalues and eigenvectors of a unitary sampled from the Haar measure, with a cost function taking, at most, the value 0.10.

B. Optimal depth

The works of [18] and [7] relate the complexity of the VQC to the amount of qubits n and depth d via $\mathcal{O}(n^3 d^2)$ and by creating a lower bound on the number of resources $R(n) \geq \text{poly}(n)$, respectively. However, such claims only provide a lower bound on the circuit complexity without ensuring a high performance. To offer a more practical understanding of the VQC complexity, we no longer treat d as being independent from n , but rather expect to find some dependence $d(n)$ for an efficient VQC performance. Recognizing this circuit behavior is essential for accurately assessing its implementability and scalability in near-term NISQ devices [19]. To formally introduce the optimal depth, we begin by defining the concept of variational unitary space:

Definition 1. *Variational Unitary Space: Space formed by all possible variational unitaries U_{VQC} attainable by a fixed architecture of the VQC $W(\hat{\theta}_j)$ with p real parameters*

$$\Gamma = \bigcup_{\hat{\theta} \in \mathbb{R}^{\times p}} \{U_{VQC}(\hat{\theta})\} \subseteq \mathbf{U}(n), \quad (1)$$

where $\mathbf{U}(n)$ represents the unitary group of $n \times n$ matrices. U_{VQC} can be described by block repetitions of length $d(n)$ which defines the depth of the VQC,

$$U_{VQC} = \prod_{j=1}^{d(n)} W(\hat{\theta}_j), \quad (2)$$

where $W(\hat{\theta}_j)$ represents a combination of parametrized single-qubit and two-qubit gates. The definition of optimal depth is subsequently formulated:

Definition 2. *Optimal depth (D_{opt}): Assuming $\exists d$ s.t. $U \subset \Gamma$, for a fixed architecture of the VQC $W(\hat{\theta}_j)$, D_{opt} is the minimal amount of layers that suffices for a fiducial reconstruction of the unitary U . More concretely, with a fixed $W(\hat{\theta}_j)$,*

$$D_{opt}(n) = \min\{d(n)\} \text{ s.t. } U_{VQC}(\hat{\theta}) \approx U. \quad (3)$$

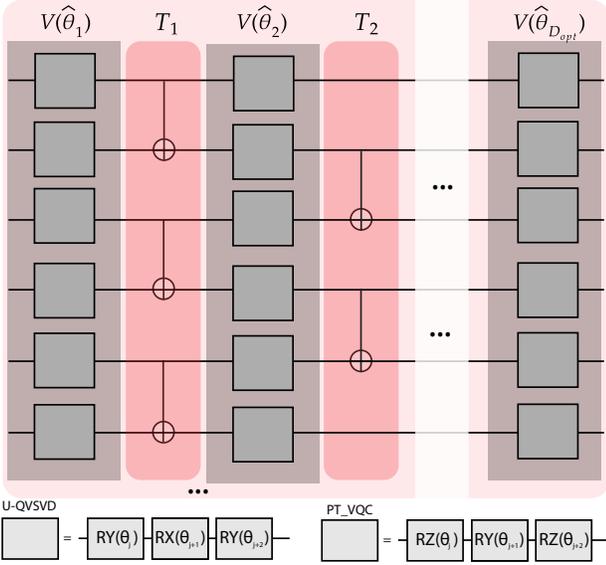


Fig. 2. Architecture of the VQC corresponding to U_{VQC} . Different single qubit gate sequences were used for PT_VQC and U-VQSVD algorithms.

For a given fixed value of n , each depth d in the VQC corresponds to the number of iterations required to achieve the target accuracy of the cost function in the PT_VQC algorithm. We search for the minimal mean number of iterations needed to attain this accuracy across 10 different target Haar random unitaries. The depth d associated to it is considered as the optimal depth D_{opt} . In the U-VQSVD scheme, instead of considering the mean number of iterations, the maximum number of iterations times d is recorded. This behavior is depicted in Fig. 1 within the context of U-VQSVD (Section III-E) for the task of reconstructing the eigenvalues and eigenvectors of 10 Haar-random unitaries.

C. PT_VQC algorithm

A new method is proposed for VQC process tomography (PT_VQC). We consider for our VQC the following parameterized architecture composed of single gate blocks $V(\hat{\theta}_j)$ and two-qubit gate blocks T_j ,

$$W(\hat{\theta}_j) = V(\hat{\theta}_j)T_j. \quad (4)$$

$U_{\text{VQC}}(\hat{\theta})$ is constructed using $d(n)$ blocks of single-qubit gate chains, comprising RZ - RY - RZ gates, and two-qubit gate blocks $T_j = CX_{\text{odd}_j|\text{even}_j}$. Here, $CX_{\text{odd}_j|\text{even}_j}$ represents a sequence of CX gates controlling either odd or even qubits, depending on the block number j .

The architecture for the VQC representing the U_{VQC} for the PT_VQC and U-VQSVD algorithms can be seen in Fig. 2 and the design of the algorithm is presented in Fig. 3. For a set of initializations completing an orthonormal basis $\{|i\rangle\}_{i=0}^{2^n-1}$, the state $|\xi\rangle$ before measurement has the form

$$|\xi\rangle = \frac{1}{2} (|\Psi_i^{\text{Pr}}\rangle + |\Psi_i^{\text{tr}}\rangle) \otimes |0\rangle + \frac{1}{2} (|\Psi_i^{\text{Pr}}\rangle - |\Psi_i^{\text{tr}}\rangle) \otimes |1\rangle, \quad (5)$$

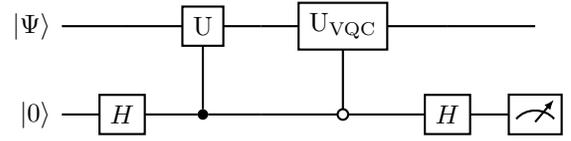


Fig. 3. Architecture for the proposed VQC tomography algorithm (PT_VQC).

where $|\Psi_i^{\text{Pr}}\rangle = U_{\text{VQC}}(\hat{\theta})|i\rangle$ and $|\Psi_i^{\text{tr}}\rangle = U|i\rangle$.

To define the subsequent partial measurement, the Von Neumann formalism is used, with the measurement projector $\Omega_0 = I \otimes |0\rangle\langle 0|$ being related to the probability p_0 of obtaining the outcome "0" in the following manner

$$\begin{aligned} p_0 &= \langle \xi | (\Omega_0)^\dagger (\Omega_0) | \xi \rangle \\ &= \frac{1}{2} - \frac{1}{2} \text{Re} \left(\langle \Psi_i^{\text{tr}} | \Psi_i^{\text{Pr}} \rangle \right). \end{aligned} \quad (6)$$

We define the cost function as

$$\begin{aligned} C(\hat{\theta}) &= \frac{1}{2^n} \sum_{i=1}^{2^n} \left\| |\Psi_i^{\text{Pr}}\rangle - |\Psi_i^{\text{tr}}\rangle \right\|^2 \\ &= \frac{1}{2^n} \sum_{i=1}^{2^n} \left(\langle \Psi_i^{\text{Pr}} | \Psi_i^{\text{Pr}} \rangle + \langle \Psi_i^{\text{tr}} | \Psi_i^{\text{tr}} \rangle \right. \\ &\quad \left. + \langle \Psi_i^{\text{Pr}} | \Psi_i^{\text{tr}} \rangle \langle \Psi_i^{\text{tr}} | \Psi_i^{\text{Pr}} \rangle \right) \end{aligned} \quad (7)$$

$$= \frac{1}{2^{n-1}} \sum_{i=1}^{2^n} [1 - \text{Re} \left(\langle \Psi_i^{\text{tr}} | \Psi_i^{\text{Pr}} \rangle \right)]. \quad (8)$$

In Appendix. A, we provide the mathematical justification for the choice of this cost function. Its computation comes from the measurement over a controlled version of the VQC, thus its gradient is computed by the 4-term shift rule [20]

$$\begin{aligned} \nabla_{\theta_i} C(\hat{\theta}) &= \frac{\sqrt{2}+1}{4\sqrt{2}} [C(\hat{\theta})|_{\theta_i=\theta_i+\frac{\pi}{2}} - C(\hat{\theta})|_{\theta_i=\theta_i-\frac{\pi}{2}}] - \\ &\quad \frac{\sqrt{2}-1}{4\sqrt{2}} [C(\hat{\theta})|_{\theta_i=\theta_i+\frac{3\pi}{2}} - C(\hat{\theta})|_{\theta_i=\theta_i-\frac{3\pi}{2}}]. \end{aligned} \quad (9)$$

The target unitary U is sampled from the Haar measure using the QR decomposition. In the minimization process, we employ the Adam optimizer, with hyperparameters $\beta_1 = 0.8$ and $\beta_2 = 0.999$, which respectively denote the decay rates of the first and second-moment estimates. In Appendix. A, we present the pseudo-code summarizing the algorithm routines for PT_VQC.

D. PT_VQC comparison to QDNN and Tensor Networks

In this section, we outline the methodology utilized for comparing PT_VQC, QDNN [3] and tensor networks [4] using MPOs. We set the number of iterations to 60 and establish the target average fidelity as

$$F = \frac{1}{2^n} \sum_{i=1}^{2^n} \left(\text{tr} \sqrt{\sqrt{\rho_i} \sqrt{\rho_i} \sqrt{\rho_i}} \right)^2 \geq 0.9, \quad (10)$$

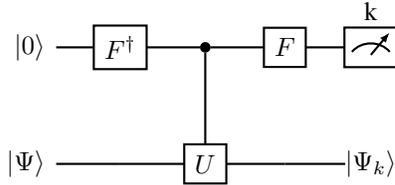


Fig. 4. PE-QPUF architecture: For a target t qubit initialization $|\Psi\rangle$ and an ancilla a qubit initialization $|0\rangle$, a set of classical outputs k and partially measured states $|\Psi_k\rangle$ are generated. During user verification, the partially measured state $|\Psi_k\rangle$ is initialized, and the new classical output k' is compared to the one generated during initialization k by the trusted party. U defines the target unitary, and F represents the quantum Fourier transform, which, abusing notation, maps $|j\rangle \mapsto \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{\frac{2\pi i j k}{2^n}} |k\rangle$.

where ρ and ρ' represent the density matrices of the ideal and predicted output states, respectively. It is important to note that we solely rely on fidelity as a metric for comparing PT_VQC to tensor networks and QDNN. The former cost function definitions remain consistent for the PT_VQC and U-VQSVD algorithms. Afterwards, we determine the minimum input state requirements for each algorithm ensuring the proper minimization of the cost function. To ensure the robustness of our results, we assess these requirements across 5 different seeds and calculate their standard deviations.

For variational tensor networks [4], the cost function relies on minimizing the Kullback-Leibler divergence [21]. The strategy behind this algorithm is to construct the MPO representation of U , assuming structures with low entanglement degrees. During each training step, we evaluate the fidelities between the predicted and actual state vectors. Employing a batch size of 10 samples, we utilize Symmetric Informationally Complete Positive Operator-Valued Measures [22] (SIC POVMs), producing 4^n state initializations.

For QDNN [3], the cost function is defined by the fidelity between the QDNN output ρ_x^{out} and the correct output ϕ_x^{out} averaged over the training data size N

$$C_{QDNN} = \frac{1}{N} \sum_{x=1}^N \langle \phi_x^{\text{out}} | \rho_x^{\text{out}} | \phi_x^{\text{out}} \rangle. \quad (12)$$

To meet the criterion of achieving a fidelity of 0.9 across 5 consecutive seeds, we utilize 3^n initial states for the QDNN scheme.

E. U-VQSVD algorithm

In this section, we introduce the U-VQSVD algorithm, drawing inspiration from the method for singular value decomposition of a unitary U delivered by [17]. Similar to the unitary process tomography discussed in Section III-C, the architecture of $U_{\text{VQC}}(\hat{\theta})$ follows that of PT_VQC, with the only change being the sequence of single-qubit gate chains, now arranged as $RY-RX-RY$ as depicted in Fig. 2.

Using the U-VQSVD scheme, we propose a new method for process tomography for unknown general channels assuming that the corresponding eigenstates can be learned up to a phase. As a demonstration of the U-VQSVD performance

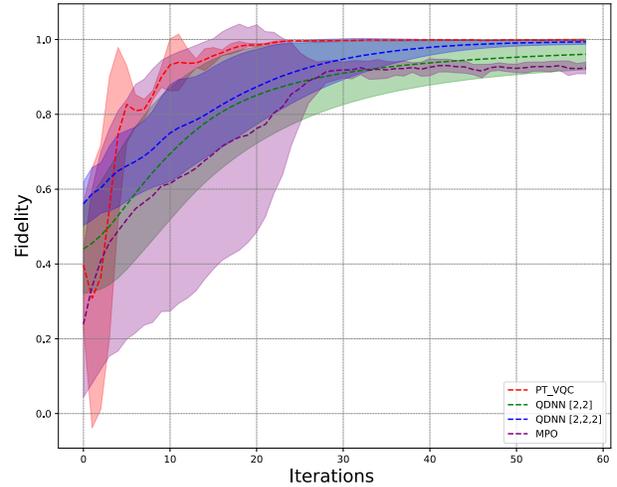


Fig. 5. Comparison between PT_VQC for 2 qubits with variational MPO and QDNN with (blue) and without (green) a hidden layer in the structure. We compute the standard deviation based on 5 different Haar random unitaries.

we conduct a forgery attempt on a PE-QPUF [16], with its architecture depicted in Fig. 4. The PE-QPUF is constructed with a Haar-random unitary U which, in the user verification stage, probabilistically yields a classical output k' close to the one generated during generation, k [16]. Both stages, generation and verification, are constructed using the quantum phase estimation algorithm. Consequently, the architecture comprises two subsets of qubits: ancillary and target qubits. Fig. 4 illustrates the circuit responsible for generating the initial classical output k with respective quantum state $|\psi_k\rangle$ to be acquired by the user. Conversely, during verification, the post-measurement state obtained during the generation serves as the input for the target system. Typically, the initialization state is not an eigenstate of U due to its Haar-random nature.

F. U-VQSVD attack on PE-QPUF

We outline the steps employed by U-VQSVD to numerically execute an impersonation attack on the PE-QPUF authentication protocol:

- 1) We start by preparing 2^n states completing the computational basis $\{|i\rangle\}_{i=0}^{2^n-1}$ and evolve each of them via the VQC U_{VQC} , using the same methodology as for the PT_VQC algorithm in Section III-C.
- 2) The cost function, instead of being defined with two independent VQCs, as in the work of [17], is just defined with one

$$C(\hat{\theta}) = \frac{1}{2^n} \sum_{i=0}^{2^n-1} 1 - \left| \langle i | U_{\text{VQC}}(\hat{\theta})^\dagger U U_{\text{VQC}}(\hat{\theta}) | i \rangle \right|. \quad (13)$$

Using the modified definition in Eq.13, the cost of the gradient computation complexity is reduced. This is achieved as the objective has changed, from ideally reconstructing the singular vectors of U , to learning them up to a global phase.

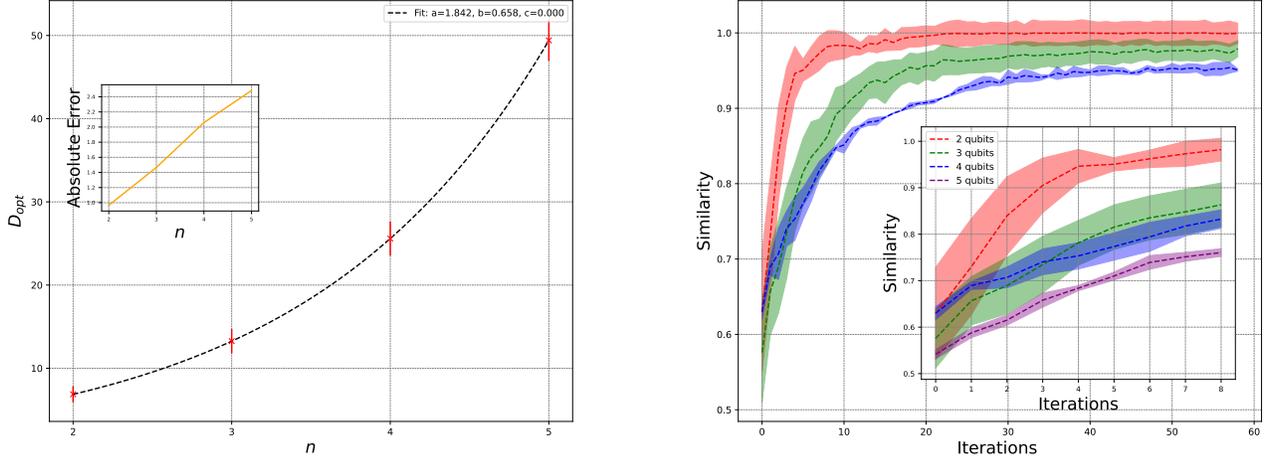


Fig. 6. Process tomography performance (PT_VQC): Left) Optimal depth (D_{opt}) fit for the minimal resources needed to achieve maximum fidelity with the respective absolute error. Right) Similarity for 5 different Haar-random unitaries per qubit in terms of the training iteration number.

- 3) The parameters $\hat{\theta}$ of the VQC are updated using the Adam optimizer. Consequently, we obtain $\{|\phi_i\rangle\}_{i=0}^{2^n-1}$ as the estimated singular vectors of U , where $|\phi_i\rangle = U_{VQC}(\hat{\theta})|i\rangle$ and $e^{i\phi_i} = \langle i|U_{VQC}(\hat{\theta})^\dagger U U_{VQC}(\hat{\theta})|i\rangle$ is the i -th estimated singular value.
- 4) Once the singular values and vectors of U have been learned, the attack occurs during the verification stage. The objective of the attacker is to impersonate the user by sending the learned singular state $|\phi_i\rangle$, corresponding to the complex phase ϕ_i which minimizes the quantity $\left| \frac{\phi_i}{2\pi} - \frac{k}{2^a} \right|$.

We assess the efficacy of this novel attack by comparing its capabilities to those of an attacker utilizing random states during the verification procedure, as well as to those of a trusted party undergoing verification.

IV. RESULTS

A. PT-VQC algorithm

In Fig. 5, we compare the performance of the PT_VQC algorithm with QDNN, both with (blue) and without (green) hidden layers [3], as well as tensor networks schemes [4]. For a scenario involving 2 qubits, with a fixed number of 60 iterations and a target fidelity of 0.9, we observe a faster convergence behavior in our scheme compared to the other two methods. It is worth noting that the attenuated oscillatory behavior observed for PT_VQC in Fig. 5 arises from the minimization problem being formulated with respect to the cost function defined in Eq. 9, which is not a monotonic function of the average fidelity.

The optimal depth of the VQC for a varying amount of qubits is presented in Fig. 6 (left). To model the relationship between the optimal depth and the number of qubits, we conducted an exponential fit of the form $D_{opt}(n) = ae^{bn} + c$, considering the standard deviation of the optimal depth, which

was calculated for 5 different Haar random unitaries U . In Fig. 6 (right), we observe the similarity, as defined in Appendix A, from 2 to 5 qubits over varying iteration numbers for 5 different Haar-random unitaries U . The performance in Fig. 6 (right) exhibits a convergent behavior, where the amplitude decreases with an increase in the number of qubits. For 5 qubits, only the first 9 iterations were generated due to high processing times. Nevertheless, Fig. 6 (left) enables us to extrapolate the optimal depth of the VQC for larger qubit sizes.

B. U-VQSVD algorithm

Following the attack presented in Section III-E, which relies on properly learning the singular values and vectors of the target unitary U of the PE-QPUF, we aim to forge the identity of 10^2 different users. We sample 10^2 Haar-random unitaries for system sizes ranging from 1 to 4 qubits. For each U , we choose 5 different ancilla sizes a ranging from 2 to 6 qubits, resulting in a total of $4 \times 5 = 20$ PE-QPUFs.

In each scenario, we conduct 25×2^a forgeries and compute the average discrepancy between the generation and verification outcomes. The data points depicted in Fig. 7 represent the mean of this average across the entire set of 10^2 different users, with the error bars indicating the fluctuations observed in the comparison across multiple users. In Fig. 7 (left), we observe the mean deviation of the U-VQSVD attack, contrasting it with Fig. 7 (right), where an attack with random initializations $|\Psi_k\rangle$ is performed during the verification. Additionally, in Fig. 7 (middle), we compare it to the reference mean deviation, where a trusted party performs the authentication.

In Fig. 7 we validate the effectiveness of the U-VQSVD targeting unknown quantum unitary evolutions. In other words, it demonstrates how an attack using our U-VQSVD algorithm, directed towards the previously defined PE-QPUF, outperforms an uninformed attack by a factor of 2 to 5 depending

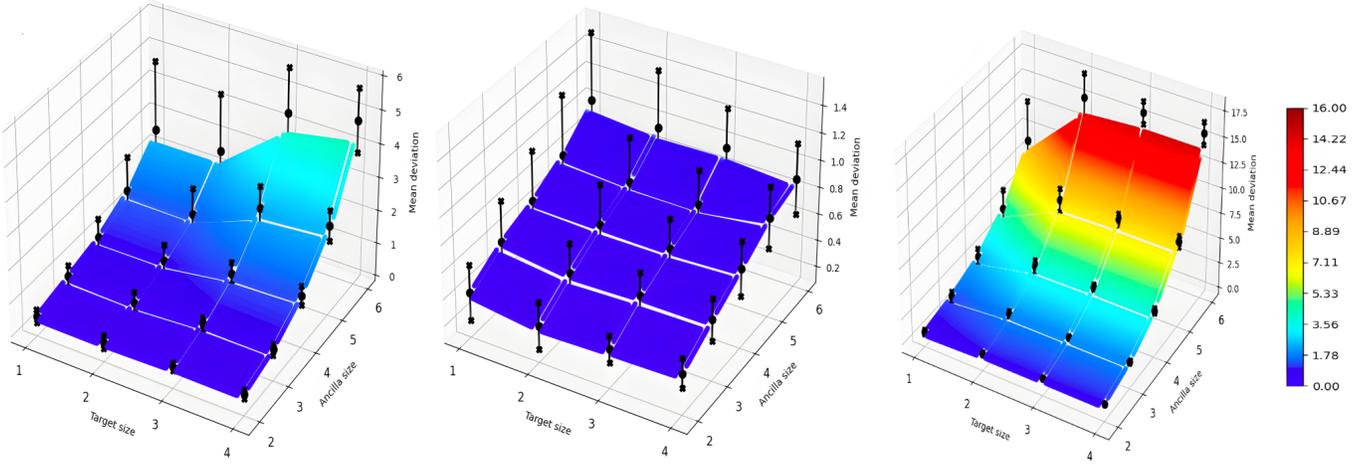


Fig. 7. SVD attack performance. The plots show the mean deviation between generation and verification outcomes for 20 different PE-QPUFs instances. Left) Displays the results coming out from the SVD attack. Middle) was obtained by simulating user-server interactions. Right) one can benchmark our attack with the performance obtained by means of a random forger, that is, always sending the state $|0\rangle^{\otimes t}$, with t being the number of target target qubits.

on the t and a sizes. It is important to note that this does not undermine the security notions established in [16]. In fact, the trusted party-server interaction demonstrates better behavior compared to our forgery attempts. For larger sizes t and a , for which security is proven to hold, our attack would already fail under its own assumptions, implying that the resources required for such a scheme scale exponentially.

V. CONCLUSIONS

In this study, we introduce two innovative process tomography techniques: PT_VQC and U-VQSVD.

PT_VQC (Section. III-C) compared to [5] significantly reduces the required number of state initializations to perform process tomography from 4^n to 2^n and halves the necessary number of qubits for each run. This enhancement results in improved algorithm processing time and increased unitary reconstruction accuracy. PT_VQC surpasses both QDNN and tensor networks (MPO), as demonstrated in Fig. 5. Unlike tensor networks utilizing MPOs, which assume low entanglement structures, PT_VQC performs well regardless of the structure of U .

U-VQSVD (Section. III-E) presents a novel process tomography scheme designed for unknown general channels. It assumes that the corresponding eigenstates can be learned up to a global phase and is based on the variational quantum singular value decomposition (VQSVD) architecture proposed in [17]. To evaluate the efficacy of the U-VQSVD algorithm, we conduct an impersonation attack on a PE-QPUF [12]. We compare the capabilities of an uninformed attacker, employing random states, with those of an attacker using U-VQSVD to generate input states, alongside a trusted party. U-VQSVD outperforms the uninformed attack by a factor of 2 to 5, depending on the ancilla and target sizes of the PE-QPUF.

It is worth noting that all the VQC employed have successfully provided solutions to the problem following a gradient-

based minimization of the cost function. We conjecture that the optimization problems posed by our cost functions, defined in Eq. 9, Eq. 13, and the parameterized ansätze are not ill-posed. In other words, they do not possess undesirable local minima. The proof supporting this conjecture may pave the way for a new theoretical research direction in VQC optimization.

APPENDIX

SIMILARITY CORRELATION TO THE COST FUNCTION

Theorem 1. *The complementary of the similarity between the target and learned operators is a monotonically increasing function of the cost defined in Eq. 9. The vanishing of the cost function defined in Eq. 9 implies a correct learning of the targeted operator.*

Proof. The complementary of the similarity, $S(A, B)$, between two operators A and B is defined via the Frobenius norm [23] as

$$1 - S(A, B) = \frac{\|A - B\|_F}{\|A\|_F}, \quad (14)$$

where, if x_{ij} are the entries of an operator X in an orthonormal basis $\{|i\rangle\}_{i=0}^{2^n-1}$, then

$$\|X\|_F = \sqrt{\sum_i \sum_j |x_{ij}|^2}. \quad (15)$$

For the unitary operators U and $U(\hat{\theta})_{\text{VQC}}$, we have

$$1 - S(U, U(\hat{\theta})_{\text{VQC}}) \propto^+ \|(U - U(\hat{\theta})_{\text{VQC}})\|_F, \quad (16)$$

where \propto^+ stands for "proportional via a positive constant". If we define $\langle k | (U - U(\hat{\theta})_{\text{VQC}}) | i \rangle \equiv \alpha_k^i$, then

$$1 - S(U, U(\hat{\theta})_{\text{VQC}}) \propto^+ \sqrt{\sum_{i=0}^{2^n-1} \sum_{k=0}^{2^n-1} |\alpha_k^i|^2}, \quad (17)$$

$$= \sqrt{\sum_{i=0}^{2^n-1} \left\| \left(U - U(\hat{\theta})_{\text{VQC}} \right) |i\rangle \right\|^2}, \quad (18)$$

leading to

$$1 - S(U, U(\hat{\theta})_{\text{VQC}}) \propto^+ \sqrt{2 \sum_{i=0}^{2^n-1} 1 - \text{Re}\{\langle i| U^\dagger U(\hat{\theta})_{\text{VQC}} |i\rangle\}}, \quad (19)$$

to finally obtain

$$1 - S(U, U(\hat{\theta})_{\text{VQC}}) \propto^+ \sqrt{f(\hat{\theta})}. \quad (20)$$

The fact that $g(x) = \sqrt{x}$ is a monotonically increasing function added to the fact that $\sqrt{0} = 0$, concludes the proof. \square

COMPUTATION OF THE REAL AND IMAGINARY PART OF AN OVERLAP BETWEEN QUANTUM STATES

Considering a Hilbert space of dimension 2^n with $|\psi\rangle, |\phi\rangle \in \mathcal{H}^{\otimes n}$. The inner product $\langle \phi | \psi \rangle$ gathers the real and imaginary parts that we want to obtain, with the assumption of owning several copies of both $|\psi\rangle$ and $|\phi\rangle$. Let V and W be unitary operators such that $V|0\rangle^{\otimes n} = |\psi\rangle$ and $W|0\rangle^{\otimes n} = |\phi\rangle$.

Real part: We can calculate the real part by carrying out the following circuit on $(n+1)$ -qubits register

$$\left(H \otimes \mathbb{1} \right) \left(C_1 W \right) \left(C_0 V \right) \left(H \otimes \mathbb{1} \right) |0\rangle_{\text{ancilla}} \otimes |0\rangle^{\otimes n}, \quad (21)$$

hence, obtaining

$$\text{Re}\{\langle \phi | \psi \rangle\} = 2p_0 - 1, \quad (22)$$

where the subscript in C_x stands for the choice of the state to be controlled and p_0 is the probability of obtaining the classical outcome "0" when measuring the ancillary qubit.

Imaginary part: We can also calculate the imaginary part by carrying out the following circuit on $(n+1)$ -qubits register

$$\left(H \otimes \mathbb{1} \right) \left(C_1 W \right) \left(C_0 V \right) \left(P \left(\frac{3}{2}\pi \right) H \otimes \mathbb{1} \right) |0\rangle_{\text{ancilla}} \otimes |0\rangle^{\otimes n}, \quad (23)$$

hence, obtaining

$$\text{Im}\{\langle \phi | \psi \rangle\} = 2p_0 - 1. \quad (24)$$

With the real and imaginary parts defined, the attacker can calculate $|\phi\rangle = W(\hat{\theta})|i\rangle$ and $|\psi\rangle = UW(\hat{\theta})|i\rangle$, in order to obtain the singular value λ_i corresponding to the i -th singular vector.

The routines for the PT_VQC algorithm are described below. Our objective is to achieve a cost function $C(\hat{\theta}) \geq 0.10$ for 5 consecutive Haar-random unitaries (with a threshold of 5). The same pseudo-code applies for U-VQSVD, but instead of the 4-term shift rule, we use the 2-term shift rule [20].

Algorithm 1 PT_VQC algorithm

```

1: Input:  $2^n$  orthogonal states,  $j = 1$ .
2: for  $j \leq$  threshold do
3:   for all iterations do
4:     Generation of a  $j$ th seed Haar-random controlled
     Unitary  $U$  as a target.
5:     for all  $\hat{\theta}$  do
6:       for all  $2^n$  do
7:         Generate 4 circuits  $U_{\text{VQC}}$  for  $\theta_i \pm \frac{\pi}{2}$  and
          $\theta_i \pm \frac{3\pi}{2}$  as seen in Fig.3.
8:         for all 4 circuits do
9:           Perform transpilation and  $m$  shot mea-
           surements.
10:        end for
11:       end for
12:       Obtain  $C(\hat{\theta})|_{\theta_i=\theta_i \pm \frac{\pi}{2}}$  and  $C(\hat{\theta})|_{\theta_i=\theta_i \pm \frac{3\pi}{2}}$  aver-
       aged over  $2^n$  states.
13:       Perform the 4-term shift rule described in
       Eq. 10.
14:     end for
15:     Obtain  $\nabla_{\theta_i} C(\hat{\theta})$  vector for all  $\theta_i$ .
16:     Use the Adam optimizer to update  $\hat{\theta}$ , for which
      $C(\hat{\theta})$  is minimized.
17:   end for
18:   if  $C(\hat{\theta}) \geq 0.10$  then
19:     Update  $D_{\text{opt}}$ .
20:      $j = 0$ .
21:   end if
22:    $j = j + 1$ 
23: end for

```

CODE AVAILABILITY

The github repository can be found at: <https://t.ly/REETC>.

ACKNOWLEDGEMENT

Christian Deppe and Roberto Ferrara were supported by the German Federal Ministry of Education and Research (BMBF), Grant 16KIS1005. Christian Deppe acknowledge the financial support by the Federal Ministry of Education and Research of Germany in the programme of "Souverän. Digital. Vernetzt". Joint project 6G-life, project identification number: 16KISK002. Vladlen Galetsky, Soham Ghosh and Christian Deppe were supported by the BMBF Project 16KISQ038. Christian Deppe and Roberto Ferrara are supported by the Munich Quantum Valley, which is supported by the Bavarian state government with funds from the Hightech Agenda Bayern Plus.

REFERENCES

- [1] S. Chen, J. Cotler, H.-Y. Huang, and J. Li, “The complexity of nisq,” *Nature Communications*, vol. 14, no. 1, p. 6001, Sep 2023. [Online]. Available: <https://doi.org/10.1038/s41467-023-41217-6>
- [2] K. Bharti, A. Cervera-Lierta, T. H. Kyaw, T. Haug, S. Alperin-Lea, A. Anand, M. Degroote, H. Heimonen, J. S. Kottmann, T. Menke, W.-K. Mok, S. Sim, L.-C. Kwek, and A. Aspuru-Guzik, “Noisy intermediate-scale quantum algorithms,” *Rev. Mod. Phys.*, vol. 94, p. 015004, Feb 2022. [Online]. Available: <https://link.aps.org/doi/10.1103/RevModPhys.94.015004>
- [3] K. Beer, D. Bondarenko, T. Farrelly, T. J. Osborne, R. Salzmann, D. Scheiermann, and R. Wolf, “Training deep quantum neural networks,” *Nature Communications*, vol. 11, no. 1, p. 808, Feb 2020. [Online]. Available: <https://doi.org/10.1038/s41467-020-14454-2>
- [4] G. Torlai, C. J. Wood, A. Acharya, G. Carleo, J. Carrasquilla, and L. Aolita, “Quantum process tomography with unsupervised learning and tensor networks,” *Nature Communications*, vol. 14, no. 1, p. 2858, May 2023. [Online]. Available: <https://doi.org/10.1038/s41467-023-38332-9>
- [5] S. Xue, Y. Liu, Y. Wang, P. Zhu, C. Guo, and J. Wu, “Variational quantum process tomography of unitaries,” *Phys. Rev. A*, vol. 105, p. 032427, Mar 2022. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.105.032427>
- [6] S. Liu, S.-X. Zhang, S.-K. Jian, and H. Yao, “Training variational quantum algorithms with random gate activation,” *Phys. Rev. Res.*, vol. 5, p. L032040, Sep 2023. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevResearch.5.L032040>
- [7] V. T. Hai and L. B. Ho, “Universal compilation for quantum state tomography,” *Scientific Reports*, vol. 13, no. 1, p. 3750, Mar 2023. [Online]. Available: <https://doi.org/10.1038/s41598-023-30983-4>
- [8] Y. Wu, J. Yao, P. Zhang, and H. Zhai, “Expressivity of quantum neural networks,” *Phys. Rev. Res.*, vol. 3, p. L032049, Aug 2021. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevResearch.3.L032049>
- [9] N. Moll, P. Barkoutsos, L. S. Bishop, J. M. Chow, A. Cross, D. J. Egger, S. Filipp, A. Fuhrer, J. M. Gambetta, M. Ganzhorn, A. Kandala, A. Mezzacapo, P. Müller, W. Riess, G. Salis, J. Smolin, I. Tavernelli, and K. Temme, “Quantum optimization using variational algorithms on near-term quantum devices,” *Quantum Science and Technology*, vol. 3, no. 3, p. 030503, jun 2018. [Online]. Available: <https://doi.org/10.1088/2058-9565/2Faab822>
- [10] X.-L. Huang, J. Gao, Z.-Q. Jiao, Z.-Q. Yan, Z.-Y. Zhang, D.-Y. Chen, X. Zhang, L. Ji, and X.-M. Jin, “Reconstruction of quantum channel via convex optimization,” *Science Bulletin*, vol. 65, no. 4, pp. 286–292, 2020. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2095927319306413>
- [11] R. Levy, D. Luo, and B. K. Clark, “Classical shadows for quantum process tomography on near-term quantum computers,” *Phys. Rev. Res.*, vol. 6, p. 013029, Jan 2024. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevResearch.6.013029>
- [12] M. Arapinis, M. Delavar, M. Doosti, and E. Kashefi, “Quantum Physical Unclonable Functions: Possibilities and Impossibilities,” *Quantum*, vol. 5, p. 475, Jun. 2021. [Online]. Available: <https://doi.org/10.22331/q-2021-06-15-475>
- [13] B. Skoric, “Quantum readout of physical unclonable functions: Remote authentication without trusted readers and authenticated quantum key exchange without initial shared secrets,” *Cryptology ePrint Archive*, Paper 2009/369, 2009, <https://eprint.iacr.org/2009/369>. [Online]. Available: <https://eprint.iacr.org/2009/369>
- [14] N. Pirnay, A. Pappa, and J.-P. Seifert, “Learning classical readout quantum puffs based on single-qubit gates,” *Quantum Machine Intelligence*, vol. 4, no. 2, Jun. 2022. [Online]. Available: <http://dx.doi.org/10.1007/s42484-022-00073-1>
- [15] V. Galetsky, S. Ghosh, C. Deppe, and R. Ferrara, “Comparison of quantum puf models,” in *2022 IEEE Globecom Workshops (GC Wkshps)*, 2022, pp. 820–825.
- [16] S. Ghosh, V. Galetsky, P. J. Farré, C. Deppe, R. Ferrara, and H. Boche, “Existential unforgeability in quantum authentication from quantum physical unclonable functions based on random von neumann measurement,” 2024.
- [17] X. Wang, Z. Song, and Y. Wang, “Variational quantum singular value decomposition,” *Quantum*, vol. 5, p. 483, jun 2021. [Online]. Available: <https://doi.org/10.22331/q-2021-06-29-483>
- [18] Y. Liu, D. Wang, S. Xue, A. Huang, X. Fu, X. Qiang, P. Xu, H.-L. Huang, M. Deng, C. Guo, X. Yang, and J. Wu, “Variational quantum circuits for quantum state tomography,” *Phys. Rev. A*, vol. 101, p. 052316, May 2020. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.101.052316>
- [19] K. Bharti, A. Cervera-Lierta, T. H. Kyaw, T. Haug, S. Alperin-Lea, A. Anand, M. Degroote, H. Heimonen, J. S. Kottmann, T. Menke, W.-K. Mok, S. Sim, L.-C. Kwek, and A. Aspuru-Guzik, “Noisy intermediate-scale quantum algorithms,” *Reviews of Modern Physics*, vol. 94, no. 1, Feb. 2022. [Online]. Available: <http://dx.doi.org/10.1103/RevModPhys.94.015004>
- [20] D. Wierichs, J. Izaac, C. Wang, and C. Y.-Y. Lin, “General parameter-shift rules for quantum gradients,” *Quantum*, vol. 6, p. 677, mar 2022. [Online]. Available: <https://doi.org/10.22331/q-2022-03-30-677>
- [21] A. Clim, R. D. Zota, and G. Tinic, “The kullback-leibler divergence used in machine learning algorithms for health care applications and hypertension prediction: A literature review,” *Procedia Computer Science*, vol. 141, pp. 448–453, Jan 2018. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1877050918317939>
- [22] A. E. Rastegin, “Notes on general sic-povms,” *Physica Scripta*, vol. 89, no. 8, p. 085101, jun 2014. [Online]. Available: <https://dx.doi.org/10.1088/0031-8949/89/8/085101>
- [23] A. Böttcher and D. Wenzel, “The frobenius norm and the commutator,” *Linear Algebra and its Applications*, vol. 429, no. 8, pp. 1864–1885, 2008. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0024379508002772>