Quantum breakfast: Variational approach for attacking QPUFs

Pol Julià Farré

May, 2024

Outline

Outline

Authentication protocols

- **Definition:** Schemes guaranteeing a secure interaction between a user and a server, i.e., the user and only the user can access the server.

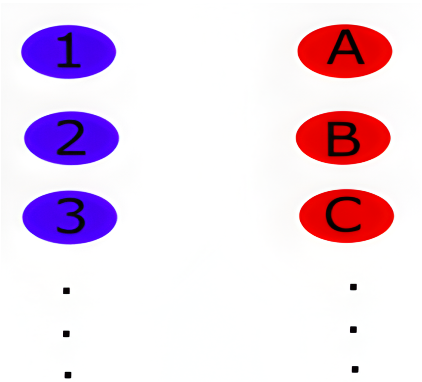
- **Token-based protocols:**

  Ownership of an object: "Something the user has."

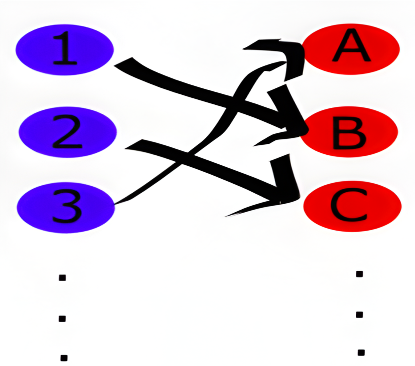
  Examples: ID card, mobile phone, etc.

  A family of tokens: Physical unclonable functions (PUFs).

PUFs: Challenge-response table



PUFs: Challenge-response table



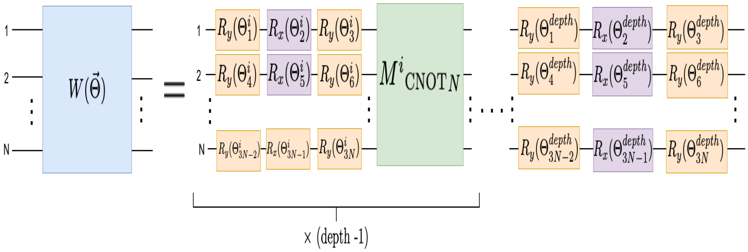
Attacking a QPUF-based authentication protocol

- **Hybrid (classical & quantum) scheme** $\rightarrow$

$\rightarrow$ Variational quantum circuits with classical optimization of a cost function.

Variational quantum circuits (VQCs)

- Fixed architecture of quantum gates.
- Free parameters.
- *depth*.



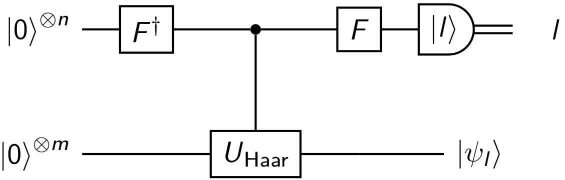
Goals

- Model two different attacks against a QPUF-based authentication protocol.
- Contribute in the research realm of variational quantum circuits.
- Produce a non-trivial bound on the performance of an optimal attack against the protocol at issue.

Outline

Phase Estimation QPUF (PE-QPUF)

- Quantum Phase Estimation circuit, revisited.



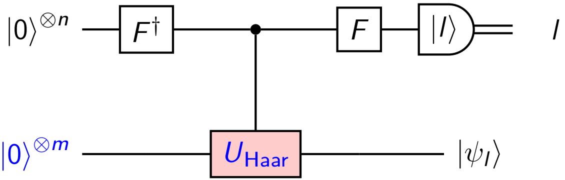
, (1)

where,

$$CU_{\text{Haar}} \equiv \sum_{k=0}^{2^n-1} |k\rangle \langle k| \otimes {U^k}_{\text{Haar}} \tag{2}$$

Phase Estimation QPUF (PE-QPUF)

- Quantum Phase Estimation circuit, revisited.



, (3)

where,

$$CU_{\text{Haar}} \equiv \sum_{k=0}^{2^n-1} |k\rangle \langle k| \otimes U^k{}_{\text{Haar}} \tag{4}$$

Stages of the protocol: Token generation

- Needed resources:

  Haar-random unitary: U_{Haar}.

  Initialization state: $|0\rangle^{\otimes n+m} = \underbrace{|0\rangle^{\otimes n}}_{\text{Ancillary}} \otimes \underbrace{|0\rangle^{\otimes m}}_{\text{Target}}$.

- Procedure:

  Send the initialization state through the Quantum Phase Estimation circuit.

  Store:

  - Classical outcome: l.
  - Post measurement (generated) state: $|\psi_l\rangle$.

Stages of the protocol: Token verification

- Protocol:

Store k_{token} generated states $\{|\psi^{i}_{l_i}\rangle\}_{i=1}^{k_{\text{token}}}$ ("challenges").

Send them through the Quantum Phase Estimation circuit.

At least one of the k_{token} classical outcomes obtained ("responses") within $[l_i - \Delta, l_i + \Delta]$.

If the classical outcome coincides with the generation one: The state can be given back to the user for a further verification (reusability).

Else: Generate a new token.

Proofs: Outcomes

Consistency proof: $m = 3n \quad \& \quad 2^n \gg 1 \implies$
The user will be accepted.

Reusability proof: The token may be reused.

Security proof: $m = 3n \quad \& \quad 2^n \gg 1$.

Drawbacks of the protocol

- Ideal assumption: Haar randomness: exponentially, in $\underline{m}$ (target size), hard to sample.

- Exponential, in $\underline{n}$ (ancillary size), depth of the Quantum Phase Estimation circuit.

Alternative:

$\rightarrow$ Heisenberg model.

Alternative: Heisenberg model

- System governed by the Hamiltonian:

$$H_{\mathrm{Hbg}} = \sum_{i,j;\ i \neq j}^{N} J_{i,j} \vec{\sigma}_i \cdot \vec{\sigma}_j, \tag{5}$$

$$\rightarrow U_{\mathrm{Hbg}} = e^{-iH_{\mathrm{Hbg}}t}. \tag{6}$$

- Randomization by uniformly sampling $J_{i,j}$ within $[0, 1]$ and t within $[0, \pi]$.

Why the Heisenberg model?

It gives rise a to practical-to-implement unitaries distribution (not exponentially hard, <u>in m</u>, to sample).

It would help circumventing the exponential, <u>in n</u>, depth of the Quantum Phase Estimation circuit **if**:

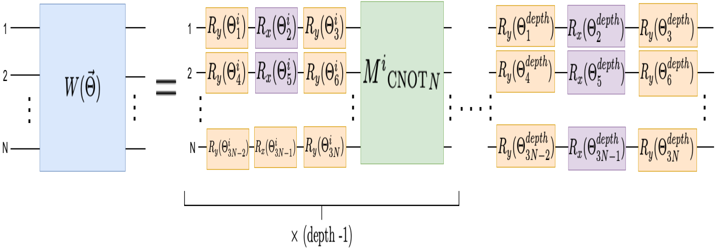
$$J_{i,j} \rightarrow 2^1 J_{i,j},\ 2^2 J_{i,j},\ \ldots,\ 2^{n-1} J_{i,j} \quad \forall i,\ j \tag{7}$$

could be experimentally achieved.

Outline

Cloning the PE-QPUF: Process tomography

- Variational quantum circuit, $W(\vec{\Theta})$, tuned towards the targeted operator: U_{Haar} [Xue et al., 2022]:



Modifications from [Xue et al., 2022]

- Cost function:

$$\mathcal{C}_{\text{Process}}(\vec{\Theta}) = 1 - \frac{1}{4^N} \sum_{i=0}^{4^N-1} \mathrm{Re}\left\{ \langle Random_j | \, U_{\text{Haar}}{}^{\dagger} W(\vec{\Theta}) \, | Random_j \rangle \right\}. \tag{8}$$

- Gradient computation via 2-terms shift rule:

$$\nabla_i C_{\text{Process}}(\vec{\Theta}) = \frac{C_{\text{Process}}(\vec{\Theta}^{+i}) - C_{\text{Process}}(\vec{\Theta}^{-i})}{2}, \tag{9}$$

where $\vec{\Theta}^{\pm i}$ shifts the i-th rotation angle by $\pm\frac{\pi}{2}$.

- Minimization of $C_{\text{Process}}(\vec{\Theta})$ via Adam optimizer.

Modifications from [Xue et al., 2022]

- Cost function:

$$\mathcal{C}_{\text{Process}}(\vec{\Theta}) = 1 - \frac{1}{2^N} \sum_{i=0}^{2^N-1} \mathrm{Re}\Big\{ \langle j| \, {U_{\text{Haar}}}^{\dagger} W(\vec{\Theta}) \, |j\rangle \Big\}. \quad (10)$$

- Gradient computation via 4-terms shift rule:

$$\nabla_i F(\vec{\Theta}) = y_1 \frac{F(\vec{\Theta}^{+i_1}) - F(\vec{\Theta}^{-i_1})}{2\sqrt{2}} - y_2 \frac{F(\vec{\Theta}^{+i_2}) - F(\vec{\Theta}^{-i_2})}{2\sqrt{2}}, \quad (11)$$

where $y_{1,2} = \frac{\sqrt{2}\pm 1}{2\sqrt{2}}$ and $\vec{\Theta}^{\pm i_1}$ shifts the i-th rotation angle by $\pm(\frac{\pi}{2} - \frac{\pi}{4})$ while $\vec{\Theta}^{\pm i_2}$ results from shifting the i-th rotation angle by $\pm(\frac{\pi}{2} + \frac{\pi}{4})$.

- Minimization of $C_{\text{Process}}(\vec{\Theta})$ via Adam optimizer.

Cloning the PE-QPUF: Insufficient

- The attacker needs to send a state.
- $\Longrightarrow$ A well suited strategy needs to be defined.

Two different attacks

Quantum state tomography (QST) attack.

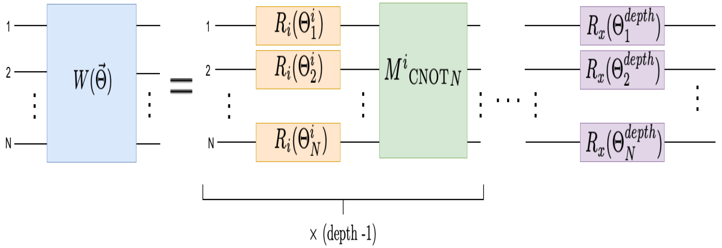
- Learning post measurement states.
- Type of queries: PE-QPUF quantum operation.

Singular value decomposition (SVD) attack.

- Learning singular values and vectors of U_{Haar}.
- Type of queries: Unitary evolution U_{Haar}.

QST

- Variational quantum circuit encoding the state ansatz [Liu et al., 2020]:



where $R_i \equiv R_y$ **if** i is even and $R_i \equiv R_x$ otherwise ($i = 0$, 1,...,$depth - 1$).

$$\rightarrow \left|\hat{\Psi}\right\rangle = W(\vec{\Theta})\,|0\rangle^{\otimes N}. \qquad (12)$$

QST attack scheme

Query the QPUF Q-many times.

Group states falling into same classical outcome.

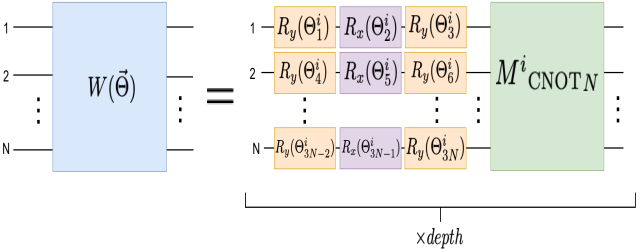
Build a reconstruction for each possible classical outcome (QST).

In the verification stage:

Send the learnt state corresponding to the generated outcome, l.

SVD

- Variational quantum circuit encoding the singular value decomposition ansatz of an N-qubits unitary, V [Wang et al., 2021]:



$$|\lambda\rangle_j = W(\vec{\Theta})\,|j\rangle \in \mathcal{H}^{\otimes N}, \quad \lambda_j = \langle j|\, W^\dagger(\vec{\Theta})\, U_{\mathrm{Haar}} W(\vec{\Theta})\,|j\rangle \in \mathbb{C}. \tag{13}$$

SVD: Modifications from [Wang et al., 2021]

- Cost function:

$$\mathcal{C}_{\mathsf{SVD}}(\vec{\Theta}) = 1 - \frac{1}{2^N}\sum_{i=0}^{2^N-1} \mathrm{Re}\left\{ \langle j|\, Z^\dagger(\vec{\Theta}) U_{\mathrm{Haar}} W(\vec{\Theta})\, |j\rangle \right\}. \quad (14)$$

- Gradient computation via 4-terms shift rule:

$$\nabla_i F(\vec{\Theta}) = y_1 \frac{F(\vec{\Theta}^{+i_1}) - F(\vec{\Theta}^{-i_1})}{2\sqrt{2}} - y_2 \frac{F(\vec{\Theta}^{+i_2}) - F(\vec{\Theta}^{-i_2})}{2\sqrt{2}}, \quad (15)$$

  where $y_{1,2} = \frac{\sqrt{2}\pm 1}{2\sqrt{2}}$ and $\vec{\Theta}^{\pm i_1}$ shifts the i-th rotation angle by $\pm(\frac{\pi}{2} - \frac{\pi}{4})$ while $\vec{\Theta}^{\pm i_2}$ results from shifting the i-th rotation angle by $\pm(\frac{\pi}{2} + \frac{\pi}{4})$.

- Minimization of $C_{\mathsf{SVD}}(\vec{\Theta})$ via Adam optimizer.

SVD: Modifications from [Wang et al., 2021]

- Cost function:

$$\mathcal{C}_{\mathrm{SVD}}(\vec{\Theta}) = 1 - \frac{1}{2^N} \sum_{i=0}^{2^N-1} \left| \langle j | W^{\dagger}(\vec{\Theta}) U_{\mathrm{Haar}} W(\vec{\Theta}) | j \rangle \right|. \quad (16)$$

- Gradient computation via 2-terms shift rule:

$$\nabla_i C_{\mathrm{SVD}}(\vec{\Theta}) = \frac{C_{\mathrm{SVD}}(\vec{\Theta}^{+i}) - C_{\mathrm{SVD}}(\vec{\Theta}^{-i})}{2}, \quad (17)$$

where $\vec{\Theta}^{\pm i}$ shifts the i-th rotation angle by $\pm\frac{\pi}{2}$.

- Minimization of $C_{\mathrm{SVD}}(\vec{\Theta})$ via Adam optimizer.

SVD attack scheme

Learn the singular values and vectors of U_{Haar}: $\left\{ |\phi_j\rangle, e^{i2\pi\phi_j} \right\}$

At verification stage:

Send the learnt eigenvector $|\phi_j\rangle$ minimizing the quantity:

$$\left| \frac{\phi_j}{2\pi} - \frac{l}{2^n} \right| \tag{18}$$

where $l \equiv$ outcome obtained at generation.

Optimal depth of VQCs

The *depth* fixes the final ansatz architecture.

Variable weakly addressed [Liu et al., 2020] in the state of the art.

→ Proposal: **10-Haar-random-targets experiment**.

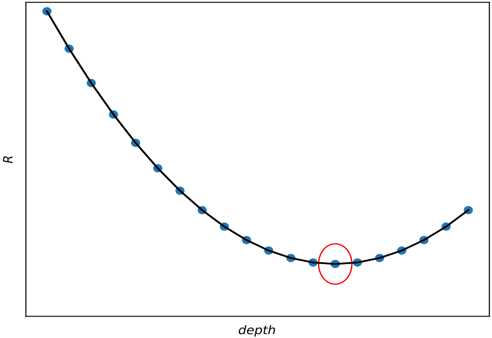
- Prepare **10 Haar-random objectives (states or SVD)**, learn them up to a certain criterion on the cost function and:

  sweep *depth*.

  Record maximum number of iterations, I_{max}, needed.

Finding the optimal depth for the VQC

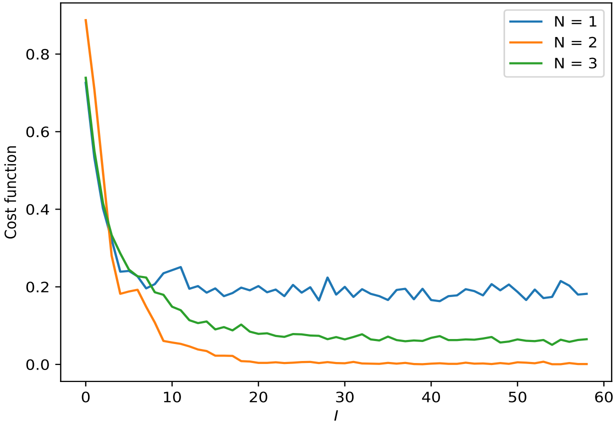
Assumption:



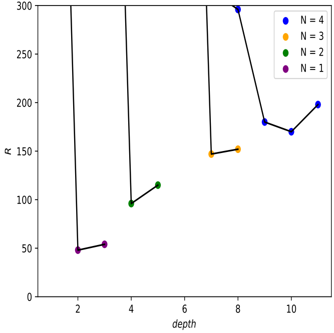
Where $R \equiv I_{\max} \cdot depth \propto \vec{\Theta}$-updates.

Outline

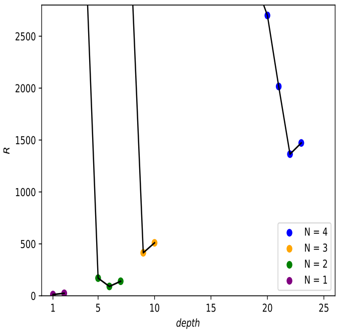
Process tomography performance



Optimal depths: how they were found

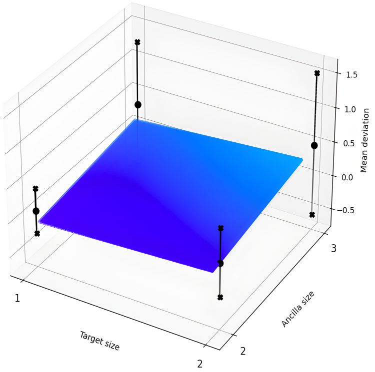


QST

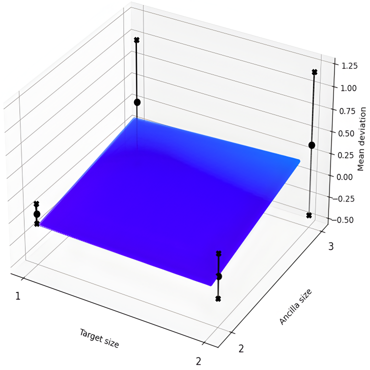


SVD

QST attack performance

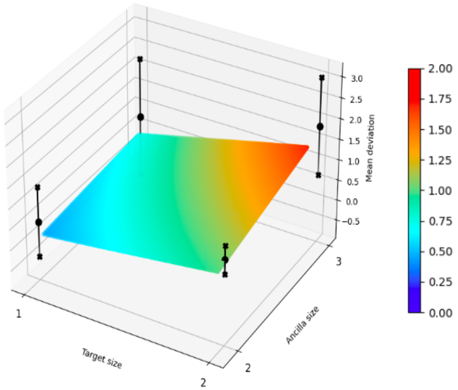


QST attack



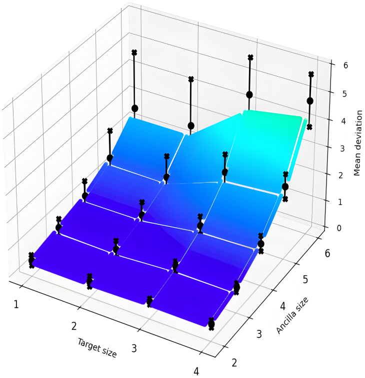
User

QST attack performance

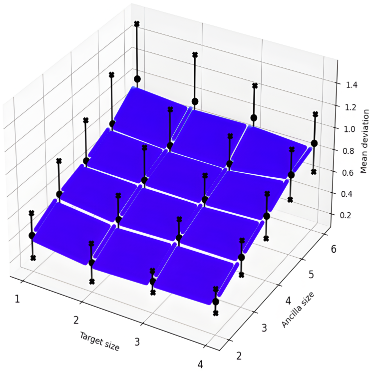


Random attack

SVD attack performance

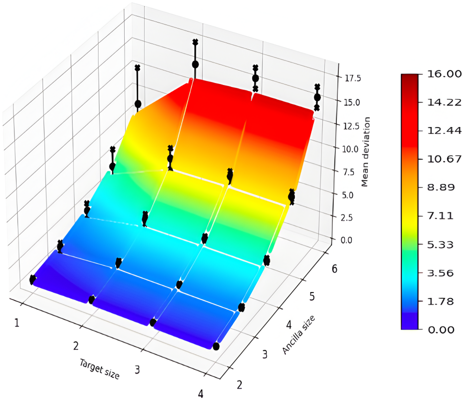


SVD attack



User

SVD attack performance



Random attack

Outline

Initial goals revisited

Model two different attacks against a QPUF-based authentication protocol.

Contribute in the research realm of variational quantum circuits.

Produce a non-trivial bound on the performance of an optimal attack against the protocol at issue.

Initial goals revisited

Model two different attacks against a QPUF-based authentication protocol. ✓

Contribute in the research realm of variational quantum circuits.

Produce a non-trivial bound on the performance of an optimal attack against the protocol at issue.

Initial goals revisited

Model two different attacks against a QPUF-based authentication protocol. ✓

Contribute in the research realm of variational quantum circuits. ✓

Produce a non-trivial bound on the performance of an optimal attack against the protocol at issue.

Initial goals revisited

Model two different attacks against a QPUF-based authentication protocol. ✓

Contribute in the research realm of variational quantum circuits. ✓

Produce a non-trivial bound on the performance of an optimal attack against the protocol at issue. ✓

Further research.

Heisenberg model.

- Experimental challenge.
- Theoretical challenge.

Noisy model.

- Bad perspectives.

Random basis measurements

- New models inspired in/resembling PE-QPUF.
- Already promising results.

Acknowledgements

Pr. Dr.
Holger Boche

Dr. Christian
Deppe

Dr. Roberto
Ferrara

Vladlen
Galetsky

Soham Ghosh

References I

Liu, Y., Wang, D., Xue, S., Huang, A., Fu, X., Qiang, X., Xu, P., Huang, H.-L., Deng, M., Guo, C., Yang, X., and Wu, J. (2020).
Variational quantum circuits for quantum state tomography.
Physical Review A, 101(5).

Wang, X., Song, Z., and Wang, Y. (2021).
Variational quantum singular value decomposition.
Quantum, 5:483.

Xue, S., Liu, Y., Wang, Y., Zhu, P., Guo, C., and Wu, J. (2022).
Variational quantum process tomography of unitaries.
Physical Review A, 105(3).

Expressibility: New definition

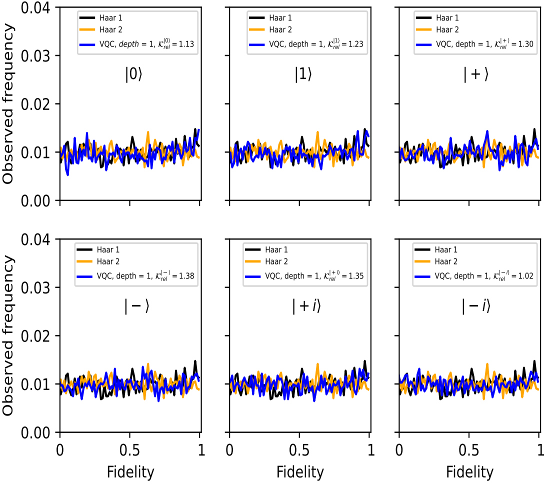
- New definition of circuit expressibility:

Sample free parameters of the VQC uniformly.

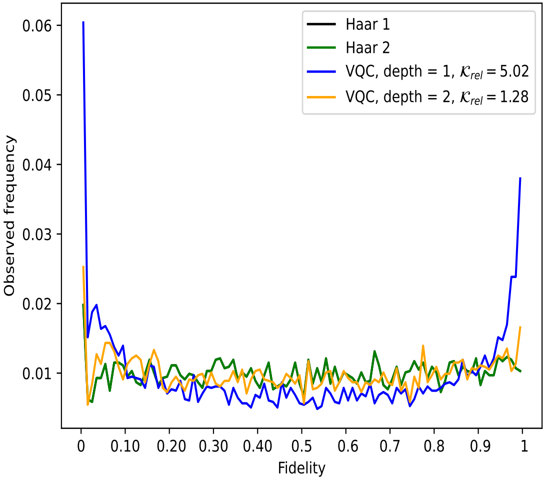
Measure "distance" towards Haar measure.

$$\mathcal{K}_{rel}(\vec{p}_{\text{vqc}}||\vec{q}_{\text{Haar-1}}) = \frac{\mathcal{K}(\vec{p}_{\text{vqc}}||\vec{q}_{\text{Haar-1}})}{\mathcal{K}(\vec{q}_{\text{Haar-2}}||\vec{q}_{\text{Haar-1}})}. \tag{19}$$

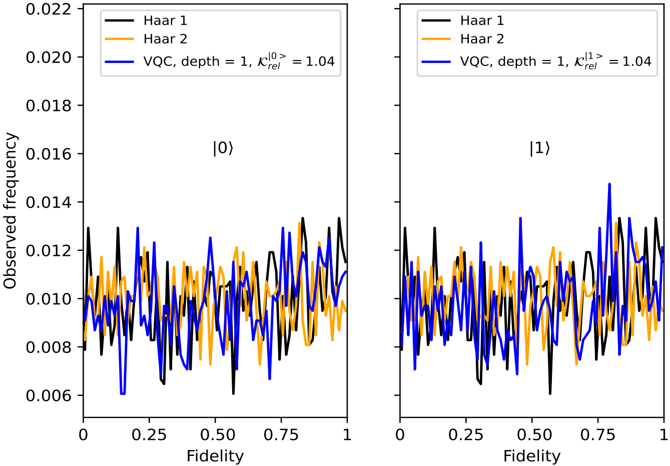
Expressibility: Process tomography



Expressibility: QST



Expressibility: SVD



Overlap computation

- Complex quantity

$$\langle\phi|\psi\rangle\,,$$

with $V\,|0\rangle^{\otimes N} = |\psi\rangle$ and $W\,|0\rangle^{\otimes N} = |\phi\rangle$.

Overlap computation

- Real part

$$\Big(H \otimes \mathbb{1}\Big)\Big(C_1 W\Big)\Big(C_0 V\Big)\Big(H \otimes \mathbb{1}\Big)\,|0\rangle_{\text{ancilla}} \otimes |0\rangle^{\otimes N}, \tag{20}$$

$$\mathrm{Re}\{\langle\phi|\psi\rangle\} = 2p_0 - 1. \tag{21}$$

Overlap computation

- Imaginary part

$$\left(H \otimes \mathbb{1}\right)\left(C_1 W\right)\left(C_0 V\right)\left(P\left(\frac{3}{2}\pi\right) H \otimes \mathbb{1}\right) |0\rangle_{\text{ancilla}} \otimes |0\rangle^{\otimes N}, \quad (22)$$

$$\mathrm{Im}\{\langle\phi|\psi\rangle\} = 2p_0 - 1. \quad (23)$$

Overlap computation

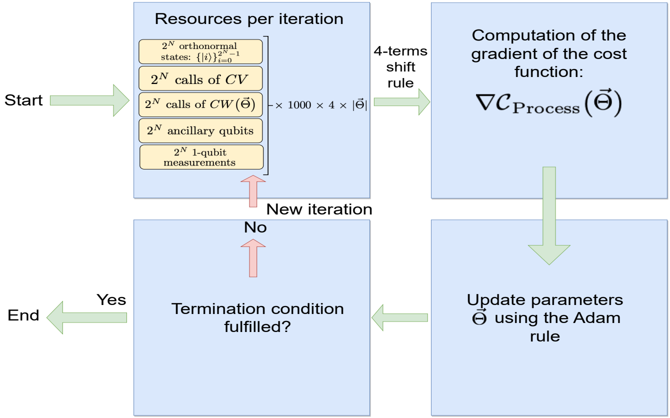
- Norm

$$\left(H \otimes \mathbb{1} \otimes \mathbb{1}\right)\left(CSWAP\right)\left(H \otimes \mathbb{1} \otimes \mathbb{1}\right) |0\rangle_{\text{ancilla}} \otimes |\psi\rangle \otimes |\phi\rangle \,, \quad (24)$$

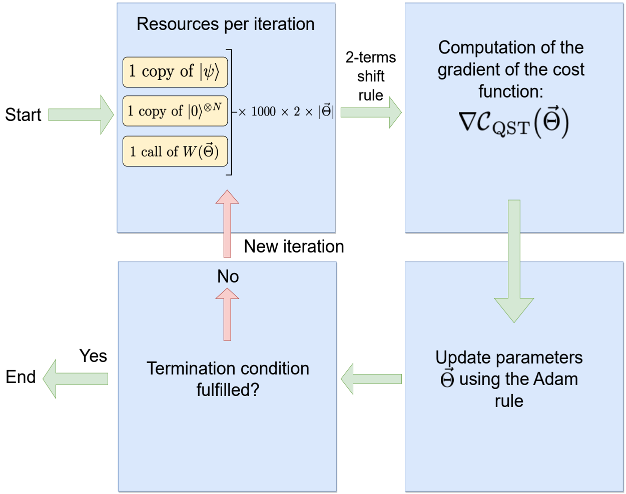
$$|\langle\phi|\psi\rangle| = \sqrt{1 - 2p_1}, \quad (25)$$

Process tomography scheme

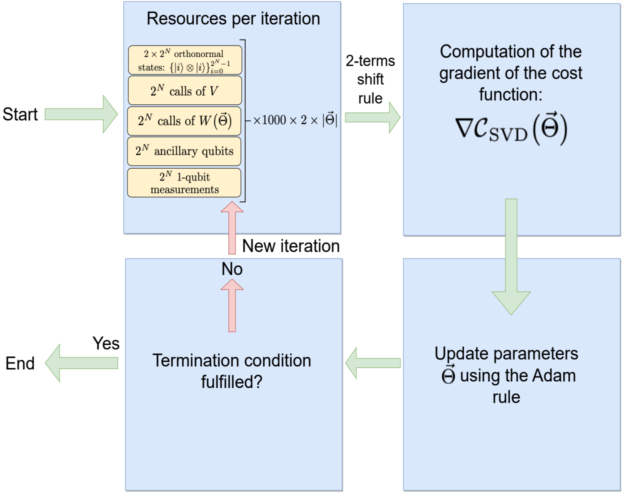
- Scheme diagram:



QST scheme


Resources per iteration
1 copy of $|\psi\rangle$
1 copy of $|0\rangle^{\otimes N}$
1 call of $W(\vec{\Theta})$
$\times\ 1000 \times 2 \times |\vec{\Theta}|$
Start
2-terms shift rule
Computation of the gradient of the cost function:
$\nabla \mathcal{C}_{\mathrm{QST}}(\vec{\Theta})$
New iteration
No
Termination condition fulfilled?
Yes
End
Update parameters $\vec{\Theta}$ using the Adam rule

SVD scheme

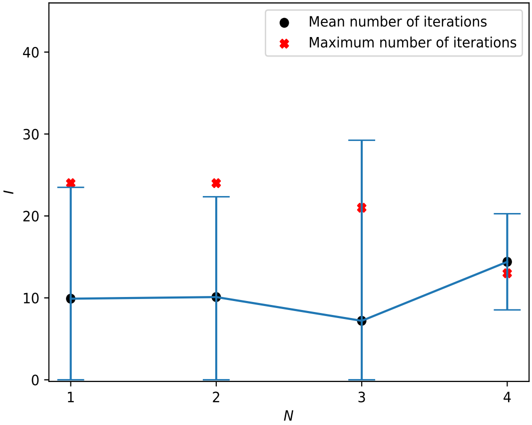

Resources per iteration
2×2^N orthonormal states: $\{|i\rangle \otimes |i\rangle\}_{i=0}^{2^N-1}$
2^N calls of V
2^N calls of $W(\vec{\Theta})$
2^N ancillary qubits
2^N 1-qubit measurements
$\times 1000 \times 2 \times |\vec{\Theta}|$
Start
2-terms shift rule
Computation of the gradient of the cost function:
$\nabla \mathcal{C}_{\mathrm{SVD}}(\vec{\Theta})$
New iteration
No
Yes
End
Termination condition fulfilled?
Update parameters $\vec{\Theta}$ using the Adam rule

QST attack: cost function

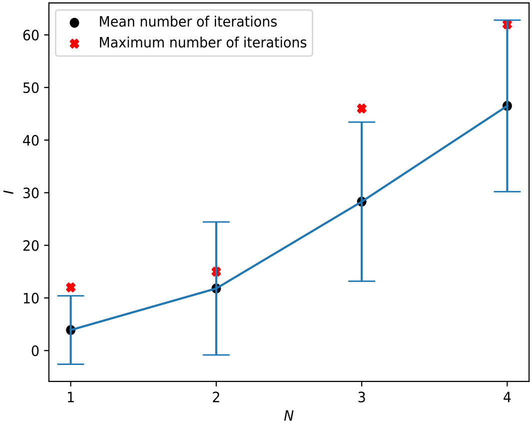
- Slight modification motivated by the inner functioning of qiskit.

$$\mathcal{C}_{\text{QST-ATTACK}} = \tilde{f}_1 = \frac{\#_1}{Q}, \tag{26}$$

QST attack: choosing number of iterations



SVD attack: choosing number of iterations

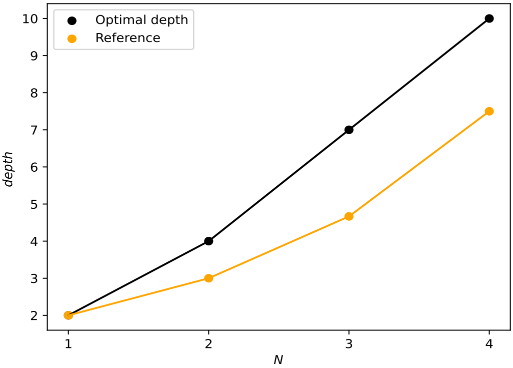


10-Haar-random-targets experiment

- QST: Learn the state $U_{\text{Haar}} |0\rangle^{\otimes N}$ up to cost function < 0.05.

- SDV: Learn SVD of the operator U_{Haar} up to cost function $<$ 0.1.

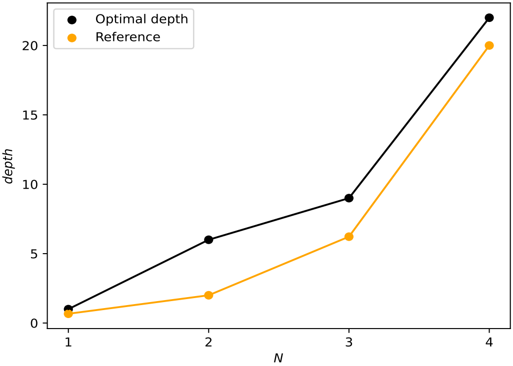
Optimal depths: derived lower bound



QST

$$\text{Lower bound}(N) = 2^{N+1} - 2$$

Optimal depths: derived lower bound



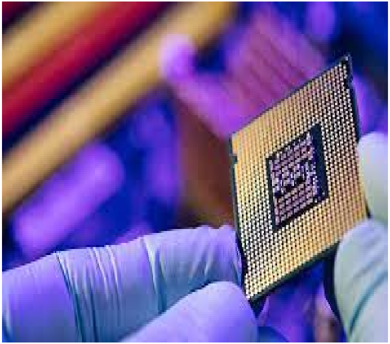
SVD

$$\text{Lower bound}(N) = 2 \cdot 2^N - 2 + 2 \cdot (2^N - 2) + \ldots 2.$$

Classical PUFs

- Classical physics are deterministic but may be too complex.

  Example of a classical PUF: Semiconductor chip.



Classical PUFs

- Classical physics are deterministic but may be too complex.

  Example of a classical PUF: Semiconductor chip.

- Randomization of characteristic properties of the chip.

  Threshold voltage.

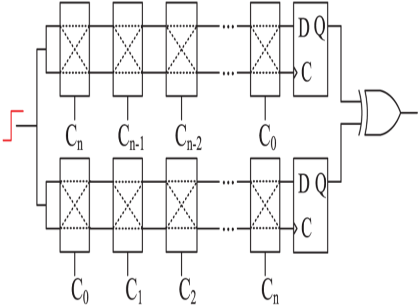
  Exact run times within a circuit.

Classical PUFs: Drawbacks

1 Need of a trusted party

Classical PUFs: Drawbacks

2 May be clonable functions → X0R-arbiter PUFs.



Proofs: Consistency proof (sketch)

The user will be accepted.

$$p_{\text{success}}(\Delta = 6)\Big|_{k_{token}=1} \geq 0.99 + \varepsilon(m, n), \tag{27}$$

$$\lim_{2^n \to \infty} \varepsilon(m = 3n, n) = 0, \tag{28}$$

$$p_{\text{success}}(\Delta = 6)\Big|_{k_{token}} \geq 1 - (1 - 0.99)^{k_{token}} \simeq 1. \tag{29}$$

Proofs: Reusability proof (sketch)

The token may be reused after verification.

$v \equiv$ number of undergone exact verifications.

$\rightarrow {p^{v+1}}_{\text{success}}(\Delta) \geq {p^{v}}_{\text{success}}(\Delta), \;\; \forall\, \Delta,\; v.$

Proofs: Security proof (sketch)

$\lambda = m = 3n$
$\downarrow$
$\underline{\text{A polynomial attacker has negligible probability of being verified}}$.

$Q \equiv$ number of PE-QPUF queries.

$\left\langle p^{\mathrm{attacker}}_{\mathrm{success}}(\Delta)\right\rangle \equiv$ expected successful attack probability.

$$Q = 0 \implies \left\langle p^{\mathrm{attacker}}_{\mathrm{success}}(\Delta)\right\rangle = \frac{2\Delta + 1}{2^{\lambda}}, \tag{30}$$

$$Q > \mathrm{poly}(\lambda)\frac{\left\langle p^{\mathrm{attacker}}_{\mathrm{success}}(Delta)\right\rangle}{(2\Delta + 1)}, \quad \forall\, \mathrm{poly}(\lambda). \tag{31}$$

Advantages of the protocol

- All stages can be public (before the attacker queries).
- Three sources of security.

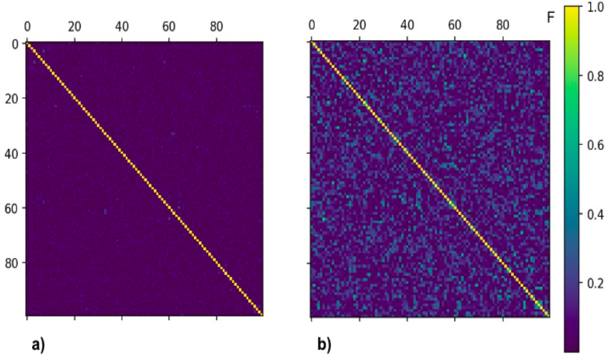
  Haar randomness: U_{Haar}.

  Quantum-measurement randomness.

  No-cloning theorem.
- Storage of only k_{token} m-qubits states required.

Haar measure vs Heisenberg model

It leads to a different PE-QPUF model.



Haar measure   Heisenberg model

Derived theoretical proofs do not apply in this case.