Title: Unclonability and How it links quantum foundations to quantum applications

Speakers: Mina Doosti

Collection: Foundations of Quantum Computational Advantage

Date: May 01, 2024 - 1:00 PM

URL: https://pirsa.org/24050025

Abstract: Quantum mechanics forbids the creation of ideal identical copies of unknown quantum systems and, as a result, copying quantum information. This fundamental and non-classical 'unclonability' feature of nature has played a central role in quantum cryptography, quantum communication and quantum computing ever since its discovery. However, unclonability is a broader concept than just the no-cloning theorem. In this talk, I will go over different notions of quantum unclonability and show how they link to many important questions and topics in quantum applications both in quantum machine learning and quantum cryptography. I will also broadly cover the link between unclonability and other fundamental concepts, such as randomness, pseudorandomness and contextuality.

Unclonability

and How it links quantum foundations to quantum applications

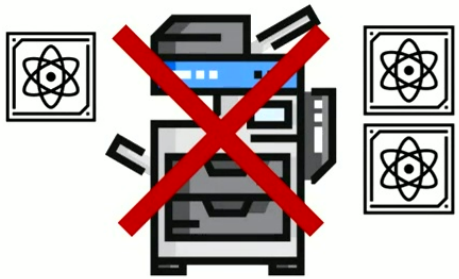
Mina Doosti

1 May 2024

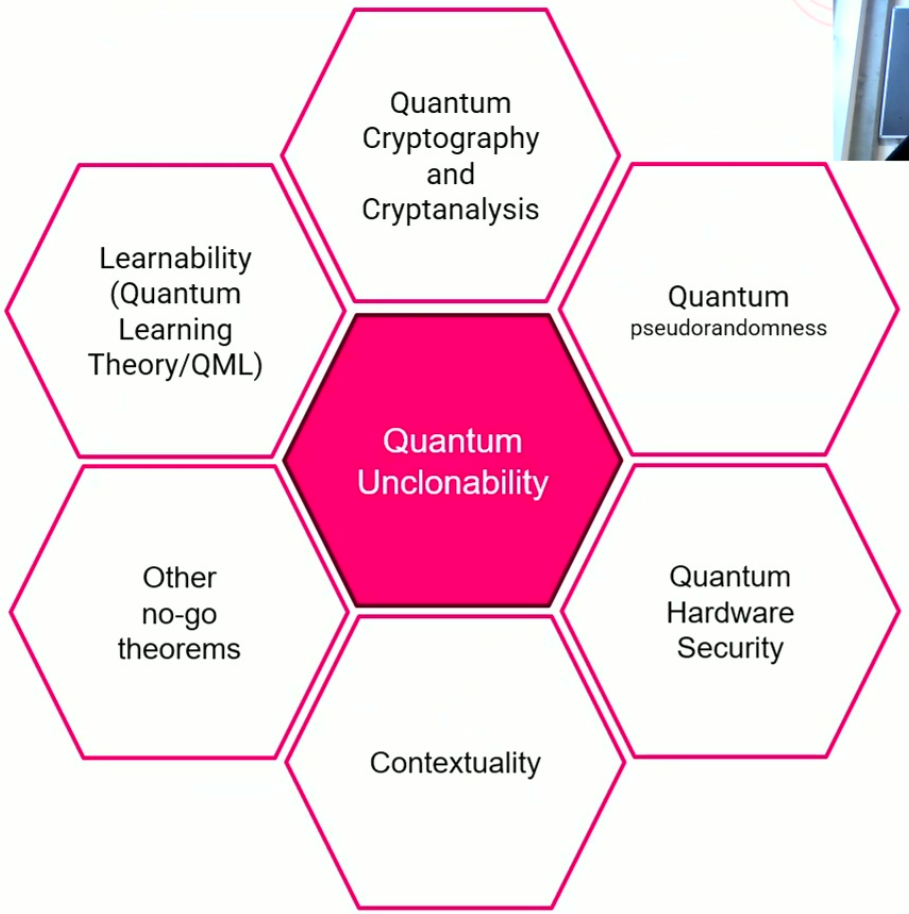
Foundations of Quantum Computing Advantage (FoQaCiA)

Perimeter Institute, Canada

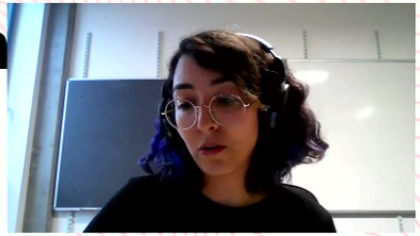
Unclonability in a broader context

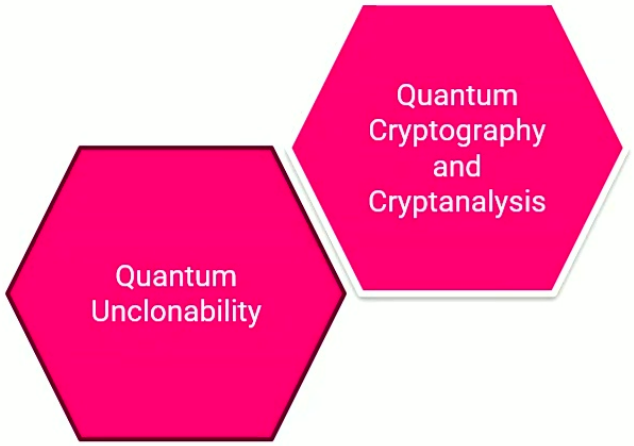


Unclonability is beyond just no-cloning theorem!



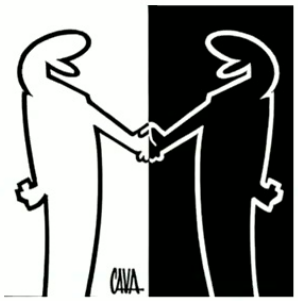
Unclonability and (more well-known) cryptograph



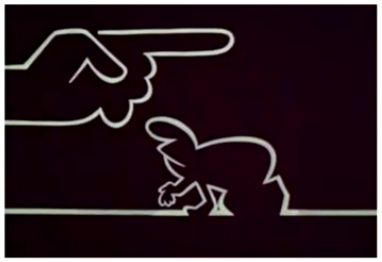


- Directly or indirectly relates to the security of most quantum protocols:
  - QKD
  - Universal Blind Quantum Computing (UBQC)
  - Quantum money
  - Quantum coin-flipping
  - …
- Quantum copy-protected software
- Unclonable Encryption
- Unclonable quantum primitives
- Quantum Zero-knowledge Proofs
- And many more!

You can’t clone and…



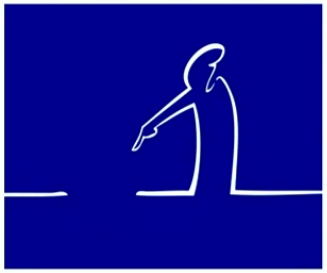
QM



Things that you can’t do!

Other no-go theorems

No-signaling

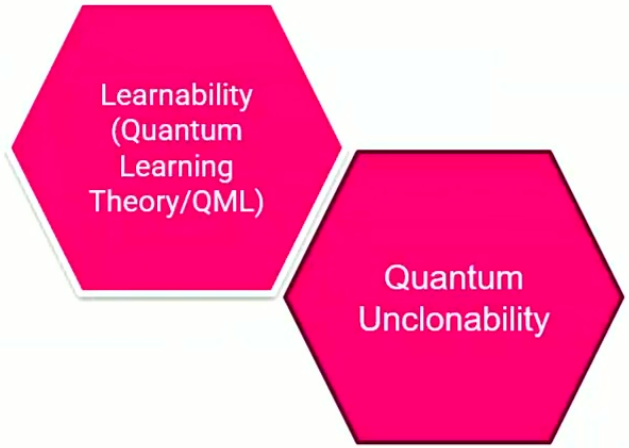


No-deleting, no-broadcasting

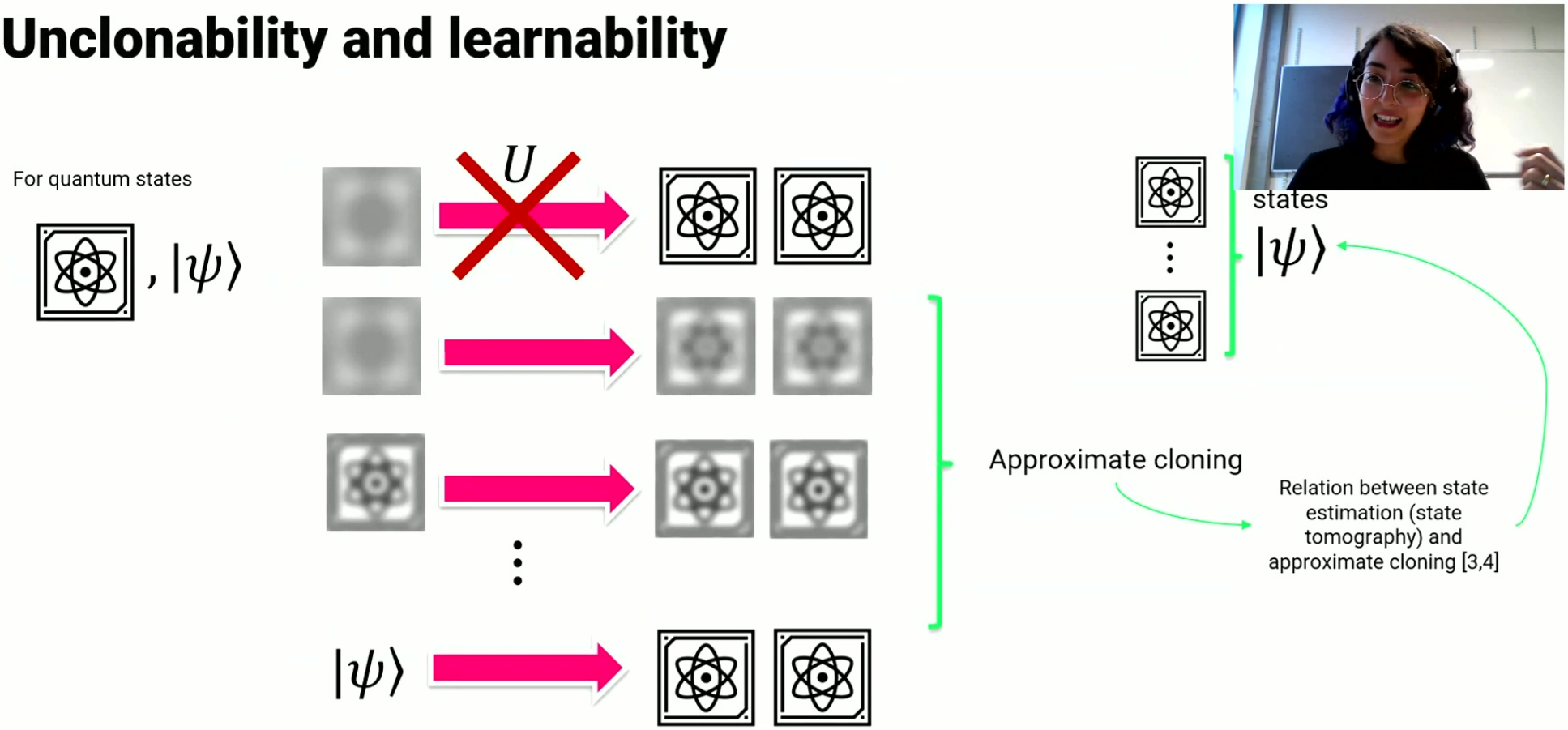
No-superposition theorems [1,2]

What else is there?!?

[1] Oszmaniec M, Grudka A, Horodecki M, Wójcik A. Creating a superposition of unknown quantum states. Physical review letters. 2016 Mar 17;116(11):110403.
[2] **Doosti M**, Kianvash F, Karimipour V. Universal superposition of orthogonal states. Physical Review A. 2017 Nov 13;96(5):052318.

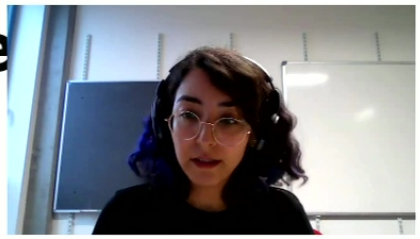

Learnability (Quantum Learning Theory/QML)
Quantum Unclonability

Unclonability and learnability



[3] Bruß, D., Ekert, A., & Macchiavello, C. (1998). Optimal universal quantum cloning and state estimation. *Physical review letters*, *81*(12), 2598.
[4] Bruß, Dagmar, et al. "Optimal universal and state-dependent quantum cloning." *Physical Review A* 57.4 (1998): 2368.

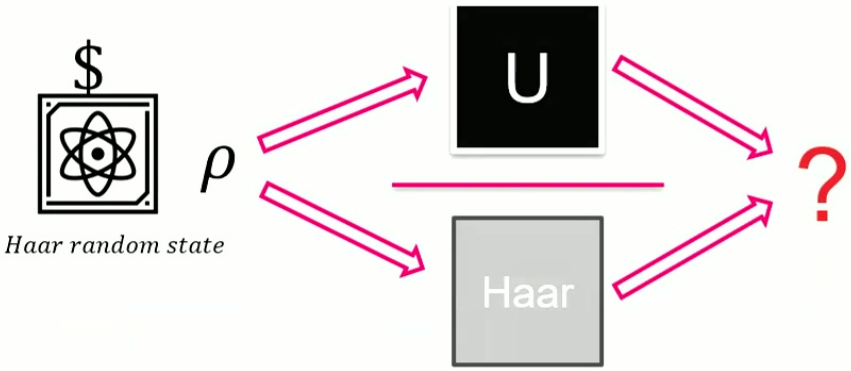
From unclonability of quantum states to processe



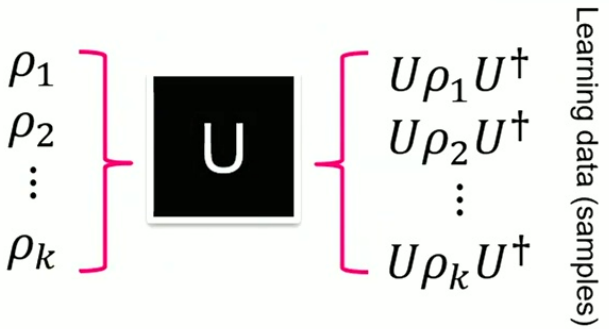
? What does “unclonability of a quantum process” mean?

First attempt [Chiribella et. al. 08]: Two black boxes O_1 and O_2 cannot be perfectly cloned by a single-use.

What about multiple-use?



“Black-box” or “Unknown” Unitary



$\rho \sim \mathcal{D} \Longrightarrow U\rho U^\dagger$

$x_\rho \Longrightarrow f(x_\rho)$

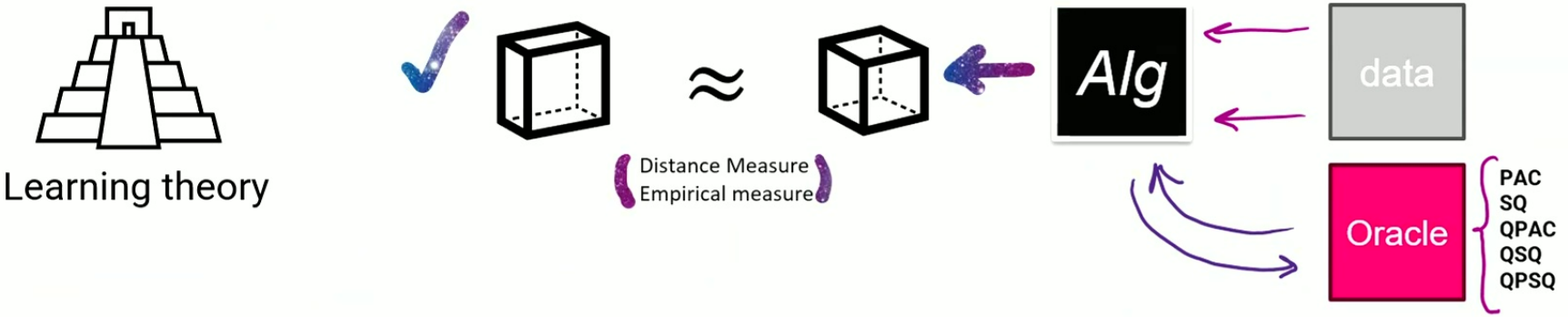
[5] Chiribella G, D'Ariano GM, Perinotti P. Optimal cloning of unitary transformation. Physical review letters. 2008 Oct 30;101(18):180504.

Unclonability and learnability

The extended notion of unclonability can be defined through the notion of “learn

Richard Feynman: *"What I cannot create, I do not understand."*

Mina/QM: *"What I cannot learn, I do not clone."*

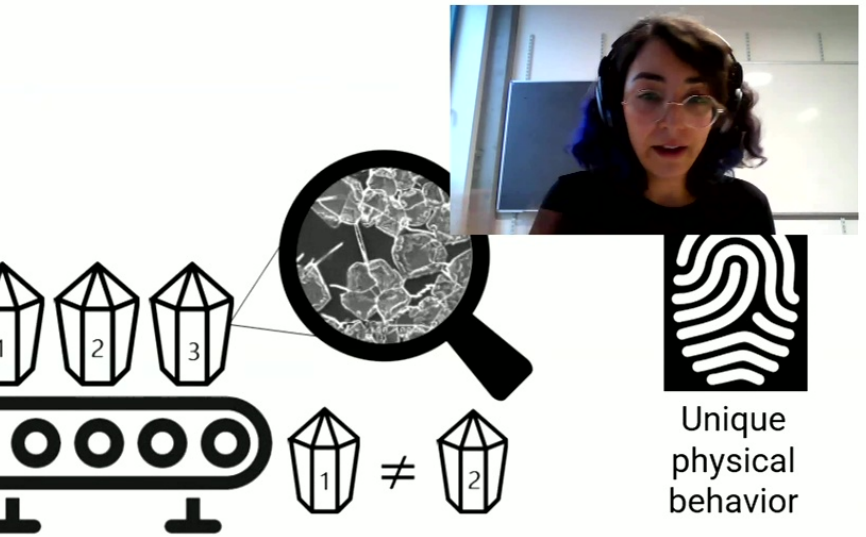


Take home message: Different flavors of unclonability can be defined based on different formal learning models.

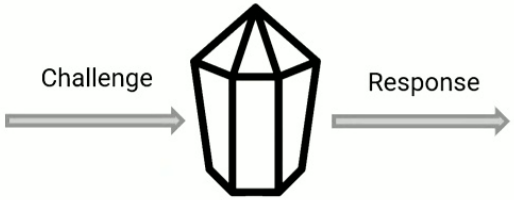

Quantum Cryptography and Cryptanalysis
Learnability (Quantum Learning Theory/QML)
Quantum Unclonability
Quantum Hardware Security

Physical Unclonability

No-cloning of quantum states is not the only type of unclonability we know!

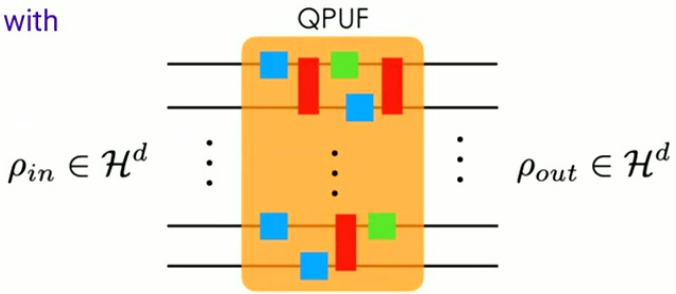


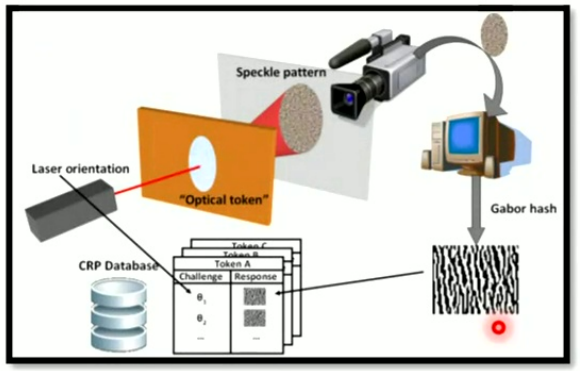
Physical Unclonable Functions (PUF)



Quantum Physical Unclonable Functions (QPUF)[6]

Unclonable (hard to clone) quantum process with quantum inputs and outputs

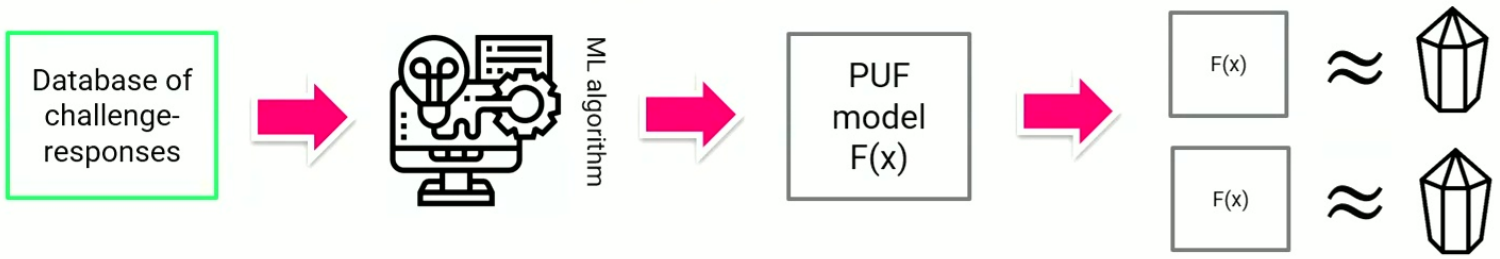




[6] Arapinis, M., Delavar, **M., Doosti**, M., & Kashefi, E. (2021). Quantum physical unclonable functions: Possibilities and impossibilities. *Quantum*, *5*, 475.

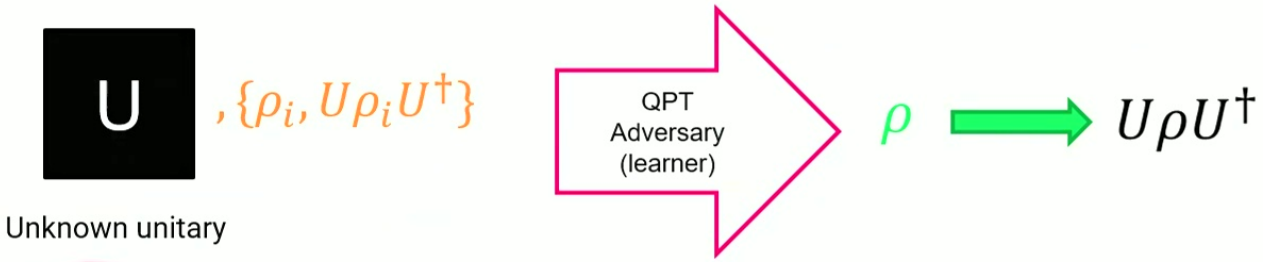
Breaking Physical Unclonability

How an unclonable hardware becomes clonable?!

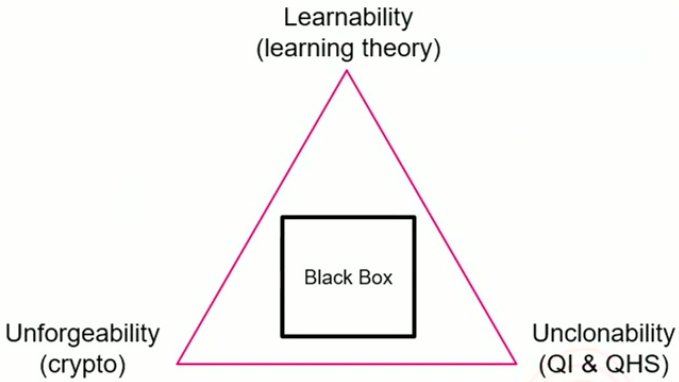


That's how you break/forge classical PUFs!

How to formalize the quantum hardware assumption of unclonability?



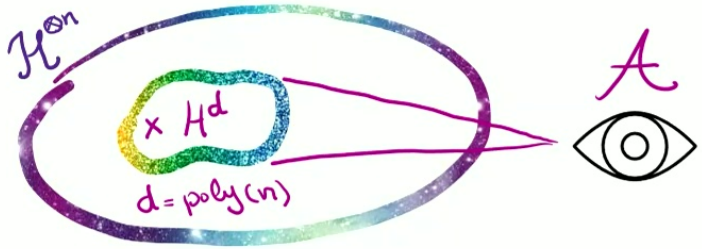
Unknown unitary



Impossibility/possibility results for security of QPU

No-Go(s)[6]:

1. **Impossibility of quantum existential unforgeability for QPUFs**
2. **Impossibility of quantum universal unforgeability for QPUFs with public DB**
3. **In general, it's impossible to have unforgeability if the target states lies in a poly-size subspace known/extractable by the adversary**



$\widetilde{\dim}(\boxed{\text{QPUF}}) \sim \exp(n)$

Possibility result[6]:
Any UQPUF (as an **unknown unitary)** can satisfy **universal unforgeability**

Provable Security (Unlike CPUF)

A unitary U which is single-shot indistinguishable to a random U (black-box) is unlearnable under Haar distribution in multi-query setting.

[7] Marvian I, Lloyd S. Universal quantum emulator. arXiv preprint arXiv:1606.02734. 2016 Jun 8.

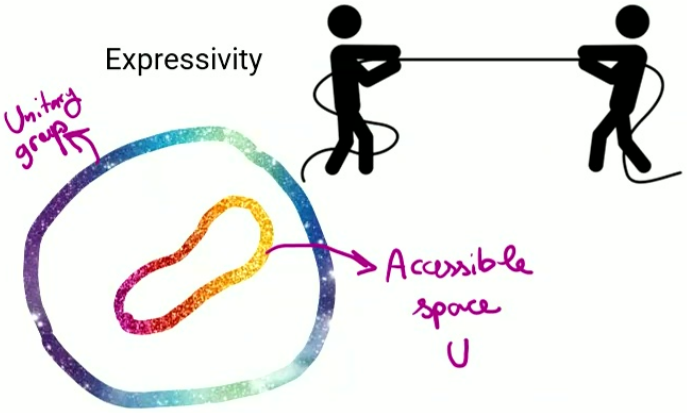
Where else do we see something like that?

In QML
Variational Quantum Algorithms

Does provable absence of barren plateaus imply
Or, why we need to rethink variational qu

M. Cerezo,[1,2,*] Martin Larocca,[3,4] Diego García-Martín,[1] N. L. Diaz,[1,5] P
Rudolph,[7] Pablo Bermejo,[8,1] Aroosa Ijaz,[3,9,10] Supanut Thanasilp,[7,11] Eric R. Anschuetz,[12,13] and Zoë Holmes[7]

[1] *Information Sciences, Los Alamos National Laboratory, Los Alamos, NM 87545, USA*
[2] *Quantum Science Center, Oak Ridge, TN 37931, USA*
[3] *Theoretical Division, Los Alamos National Laboratory, Los Alamos, NM 87545, USA*
[4] *Center for Nonlinear Studies, Los Alamos National Laboratory, Los Alamos, New Mexico 87545, USA*
[5] *Departamento de Física-IFLP/CONICET, Universidad Nacional de La Plata, C.C. 67, La Plata 1900, Argentina*
[6] *University of Strathclyde, Glasgow G1 1XQ, UK*
[7] *Institute of Physics, Ecole Polytechnique Fédérale de Lausanne (EPFL), Lausanne CH-1015, Switzerland*
[8] *Donostia International Physics Center, Paseo Manuel de Lardizabal 4, San Sebastián E-20018, Spain*
[9] *Department of Physics and Astronomy, University of Waterloo, Ontario, N2L 3G1, Canada*
[10] *Vector Institute, MaRS Centre, Toronto, Ontario, M5G 1M1, Canada*
[11] *Chula Intelligent and Complex Systems, Department of Physics, Faculty of Science, Chulalongkorn University, Bangkok, Thailand, 10330*
[12] *Institute for Quantum Information and Matter, Caltech, Pasadena 91125, USA*
[13] *Walter Burke Institute for Theoretical Physics, Caltech, Pasadena 91125, USA*



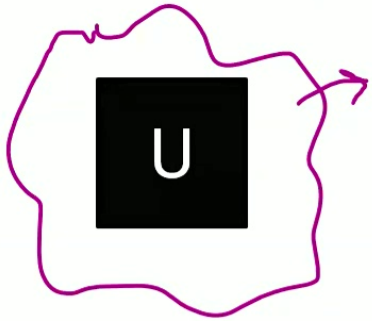
Trainability
(Barren Plateau)

stuck! $\mathrm{Var}[\partial_k C] = \frac{1}{\exp}$

Provably barren plateau-free architectures live in classically identifiable polynomial subspaces.

- Can we make formal connection between effective dimensionality of unclonable functions and expressivity?
- Does that help us to better understand quantum advantage in QML?

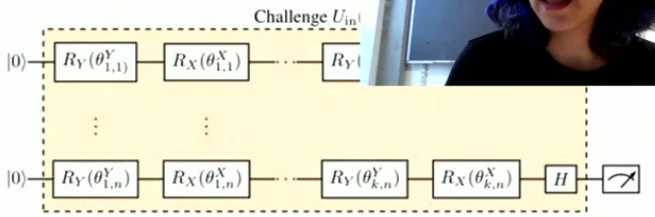
Other types of Quantum PUFs and more learning th



Noisy black box

The output is the statistics instead of the quantum states

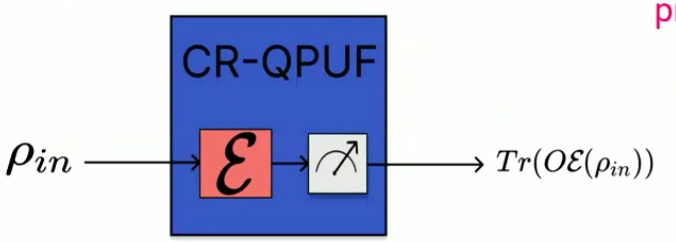
Classical readout of quantu



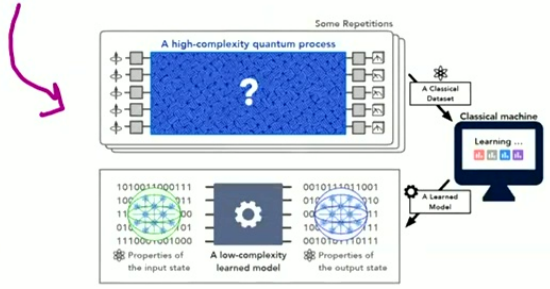
The problem is...
They are broken (using ML) [8]

But this is a very simple circuit... What if we keep this model, but the circuit it more complicated?

CR-QPUF in Statistical Query (SQ) model



We defined and studied the problem of learning quantum processes from statistical queries [2].



New algorithm in QPSQ model

This family of QPUFs are efficiently learnable (except some restricted cases, which are probably not efficient) and hence, not good candidates for unclonable processes.

[8] Pappa, Anna, Niklas Pirnay, and Jean-Pierre Seifert. arXiv:2112.06661 (2021).
[9] Huang, Hsin-Yuan, Sitan Chen, and John Preskill. "Learning to predict arbitrary quantum processes." *PRX Quantum* 4.4 (2023): 040337.
[10] Wadhwa, Chirag, and Mina Doosti. "Learning Quantum Processes with Quantum Statistical Queries." *arXiv preprint arXiv:2310.02075* (2023).


PhD Student
Image created by DALL.E

Quantum Pseudorandomness

True quantum randomness (Haar randomness)

Statistical: t-design

Approximation of Haar randomness

Computational: PRS/PRU

Pseudorandom quantum states/unitaries [Ji, Liu, Song 2018]: Set of keyed states/unitaries that can be generated efficiently and are computationally indistinguishable to Haar-random states/unitaries

Computational version of no-cloning theorem from PRS

$$|\phi_k\rangle^{\otimes m} \sim PRS \qquad |\psi\rangle^{\otimes m} \sim Haar$$

$$\mathcal{D}$$

I don't know...

Created very interesting body of research in cryptography, complexity theory, and physics (quantum gravity) over the past 6 years

Can we achieve quantum pseudorandomness under a different set of assumptions? Hardware assumptions maybe?

[11] Ji Z, Liu YK, Song F. Pseudorandom quantum states. In Advances in Cryptology–CRYPTO 2018: August 19–23, 2018.

Quantum pseudorandomness and hardware assur

Family of quantum physical unclonable functions → Family of pseudorandom quantum operations → Generators for pseudorandom quantum states → Efficient Unforgeability

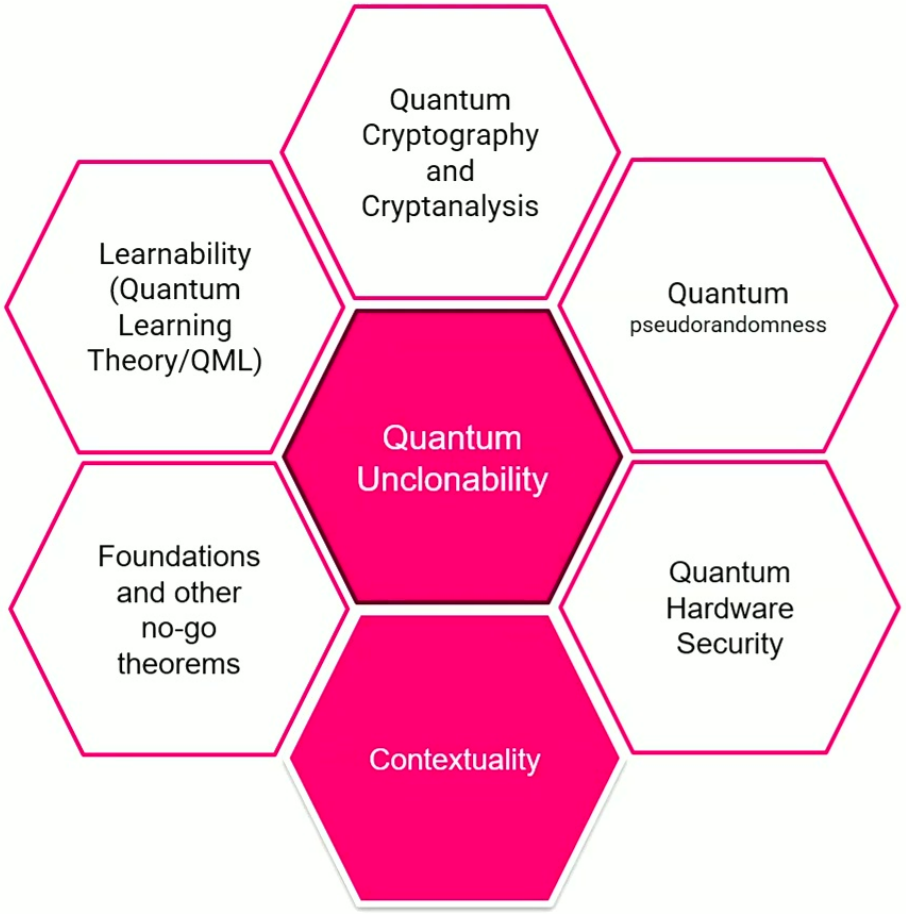
Connects hardware assumption and unclonability to computational assumption

Almost-maximal uniqueness (closed to max distance in diamond norm) → PRU

Proof toolbox from Random Matrix theory:

- We impose the $2-\epsilon$ distance in the diamond norm on the unitary set and then look at the distribution of the eigenvalues
- It has been shown (Diaconis-Shahshahani [9]) that for Haar-random matrices it converges to uniform distribution over unit circle
- We show that our maximal distinguishability condition also makes the eigenvalues to disperse uniformly on the unit circle
- We show the two distribution in the asymptotic limit converge to the same thing

[12] **Doosti, M.**, Kumar, N., Kashefi, E., & Chakraborty, K. (2022). On the connection between quantum pseudorandomness and quantum hardware assumptions. *Quantum Science and Technology*, *7*(3), 035004.
[13] Diaconis P, Shahshahani M. On the eigenvalues of random matrices. Journal of Applied Probability. 1994 Jan;31(A):49-62.


Quantum Cryptography and Cryptanalysis
Learnability (Quantum Learning Theory/QML)
Quantum pseudorandomness
Quantum Unclonability
Foundations and other no-go theorems
Quantum Hardware Security
Contextuality

Unclonability and contextuality

Is no-cloning theorem as non-classical as we think?

Well… No…

Cloning and Broadcasting in Generic Probabilistic Models

Howard Barnum[1] Jonathan Barrett[2] Matthew Leifer[2,3]
Alexander Wilce[4]

But… more generally yes!?

Contextual advantage for state-dependent cloning

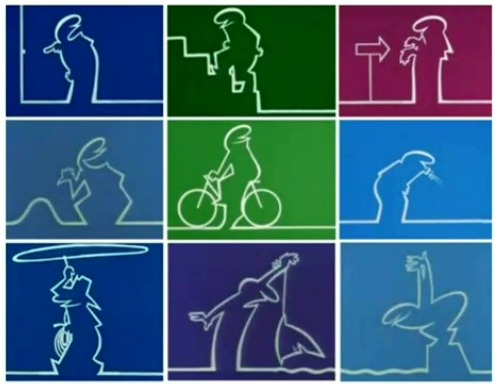
Matteo Lostaglio[1,2] and Gabriel Senno[1]

[1]ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, Castelldefels (Barcelona), 08860, Spain
[2]QuTech, Delft University of Technology, P.O. Box 5046, 2600 GA Delft, The Netherlands

So… what's going on? What about other cloning tasks?

Farid Shahandeh

ROYAL HOLLOWAY UNIVERSITY OF LONDON



"Maybe we need a new way to witness contextuality!"

Gong show talk by Farid today (Contextuality via dimension witnesses)

Applications (or Quantum advantage quest)

Extended notion of unclonability

Learning theory

Understanding QML better

Cryptography from new sets of assumptions

- wormhole growth and AdS/CFT correspondence [18]

Physics

- Crypto from blackholes! [19]
- Quantum Algorithms in a Superposition of Spacetimes [20]

Quantum Hardware Assumptions (like QPUF)

- Identification [14]
- Mutual authentication [15]
- New protocol with authentication as a subroutine (?)
- Distributed QC (?)

Quantum pseudo-randomness

- Commitment [16]
- Digital Signature [16,17]
- CPA-secure Quantum Encryption [17]
- MAC [17]

[14] **Doosti, M**, et al. "Client-server identification protocols with quantum puf." *ACM Transactions on Quantum Computing* 2.3 (2021): 1-40.
[15] Chakraborty, K., **Doosti, M**., Ma, Y., Wadhwa, C., Arapinis, M., & Kashefi, E. (2021). Quantum Lock: A Provable Quantum Communication Advantage. *arXiv preprint arXiv:2110.09469*.
[16] Morimae, Tomoyuki, and Takashi Yamakawa. "Quantum commitments and signatures without one-way functions." In Annual International Cryptology Conference, 2022.
[17] Ananth, Prabhanjan, Luowen Qian, and Henry Yuen. "Cryptography from pseudorandom quantum states." In Annual International Cryptology Conference 2022
[18] Bouland, A., Fefferman, B., & Vazirani, U. (2019). Computational pseudorandomness, the wormhole growth paradox, and constraints on the AdS/CFT duality. arXiv preprint arXiv:1910.14646
[19] Shmueli O. Quantum Algorithms in a Superposition of Spacetimes. arXiv preprint arXiv:2403.02937. 2024 Mar 5.
[20] Brakerski Z. Black-Hole Radiation Decoding Is Quantum Cryptography. InAnnual International Cryptology Conference 2023 Aug 9 (pp. 37-65). Cham: Springer Nature Switzerland.

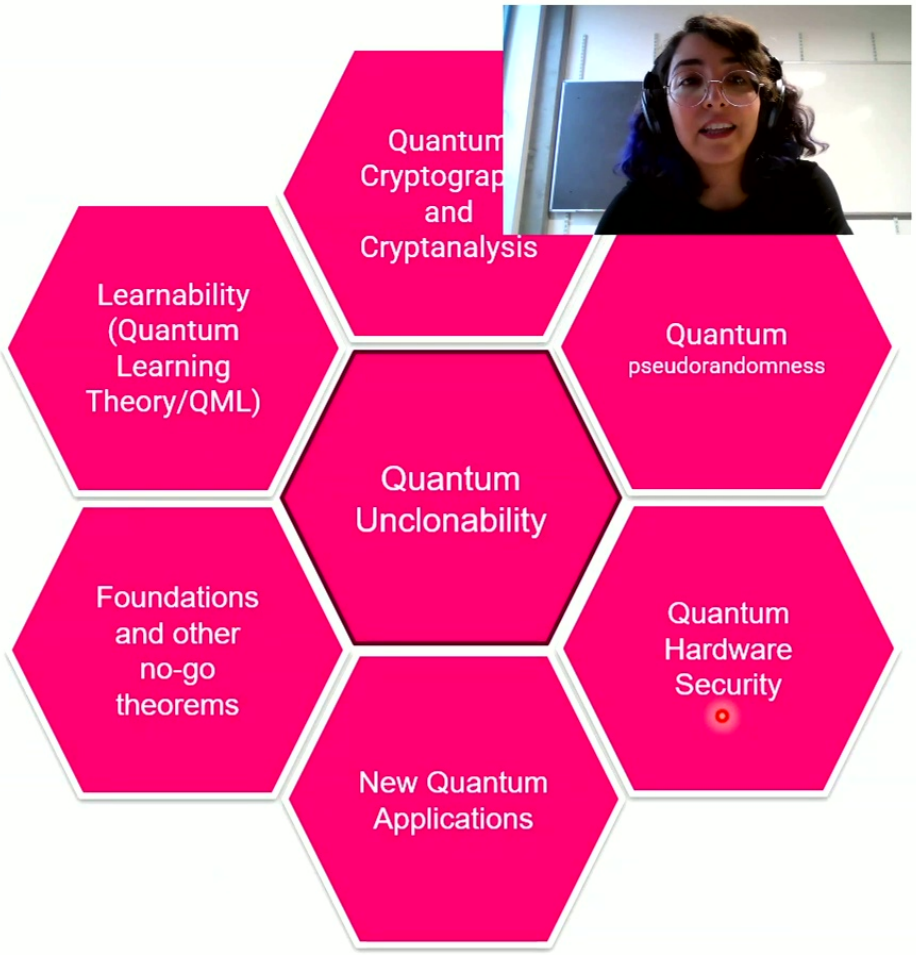
Conclusion

(Extended)Unclonability is a very interesting fundamental property to study, related to many concepts such as learnability

The study of unclonability and its relation to learning may help us to understand quantum advantage (or lack of it) in QML

Unclonable primitives (from different sets of assumptions) are useful in cryptography and tools to build cryptographic schemes with unique features (in a way, quantum advantage in crypto)

Unclonability and contextuality seems to be related in a very interesting and non-trivial way!



Thank you!

PhD Position Open in Edinburgh!

mdoosti@ed.ac.uk
minadoosti.github.io