Variational approach for attacking QPUFs

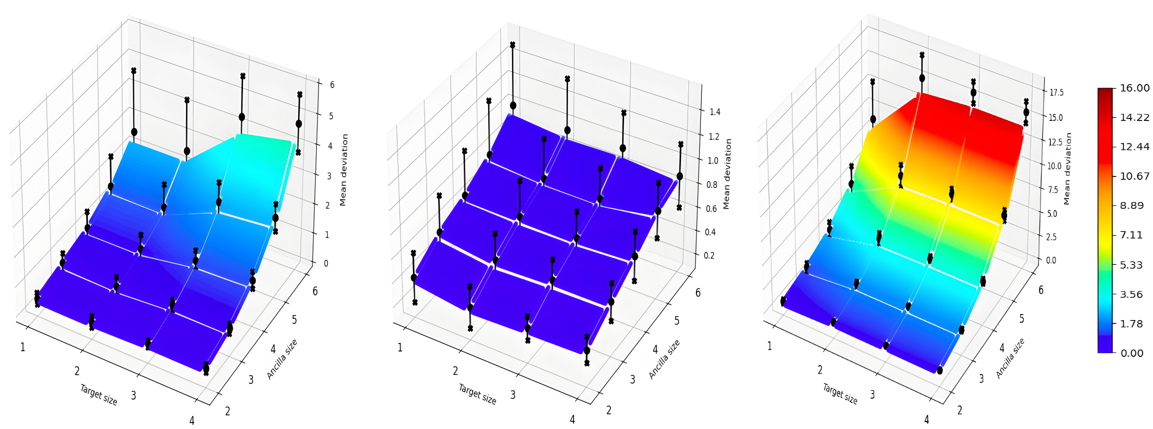
Pol Julià Farré
Technical University of Braunschweig, Braunschweig, Germany.

Utilizing the uncontrollable variations within manufacturing processes for secure authentication purposes can be already found in the works [1] and [2]. Later on, this idea was formalized by coining the term physical unclonable function (PUF) [3], leading to several proposals and patents in the subsequent years and establishing PUFs as a promising secure fingerprint. Nonetheless, classical PUFs lack fundamental security notions [4], and rely on an initial *unclonability assumption* of certain systems that may be afterwards found to be efficiently clonable [5].

In [6], a PUF design was derived by means of the quantum theory, aiming to tackle some of the stated vulnerabilities by exploiting the *no-cloning theorem* of quantum states. In the work [7], different flaws within such first quantum physical unclonable function (QPUF) were identified, and a new proposal trying to address such inconveniences was delivered: the Unkonown unitary QPUF. Finally, and being it the most recent contribution to the field at the time of writing this abstract, [8] harnessed the intrinsic random nature of quantum measurements in order to define a new QPUF model.

In this presentation we aim to

1) make the interconnection between PUFs and secure authentication comprehensible for the listeners to then present a significant contribution made to the field: modifying two existing algorithms in the state of the art of variational quantum tomography [9], [10], in order to substantially enhance their efficiency.
2) display how such modifications allowed for attacking a novel QPUF-based authentication scheme, obtaining a better performance than that one given by a randomized scheme (see Fig. 1).



(a) SVD forgery (b) User behaviour (c) Random forgery

Fig. 1: Performance of the singular value decomposition (SVD) attack. Each data point (black) corresponds to a different choice of intrinsic parameters of the simulated QPUF. Low heights are compatible with a high rate of successful authentications, while large heights correspond to denied attempts. **a** shows how our attack performs, as expected, worse than what an actual user would (**b**), but substantially better than uninformed forgeries (**c**), characterized by randomizing the attack algorithm.

References

[1] D. Bauder, *An anti-counterfeiting concept for currency systems*. Sandia National Labs., 1983.
[2] G. J. Simmons, "A system for verifying user identity and authorization at the point-of sale or access," *Cryptologia*, vol. 8, no. 1, pp. 1–21, 1984.
[3] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.
[4] C. Helfmeier, C. Boit, S. Tajik, and J.-P. Seifert, "Physical vulnerabilities of physically unclonable functions," pp. 1–4, 01 2014.
[5] G. Becker, "The gap between promise and reality: On the insecurity of xor arbiter pufs," vol. 9293, pp. 535–555, 09 2015.
[6] 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.
[7] M. Arapinis, M. Delavar, M. Doosti, and E. Kashefi, "Quantum physical unclonable functions: Possibilities and impossibilities," *Quantum*, vol. 5, p. 475, June 2021.
[8] 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.
[9] S. Xue, Y. Liu, Y. Wang, P. Zhu, C. Guo, and J. Wu, "Variational quantum process tomography of unitaries," *Physical Review A*, vol. 105, Mar. 2022.
[10] X. Wang, Z. Song, and Y. Wang, "Variational quantum singular value decomposition," *Quantum*, vol. 5, p. 483, June 2021.