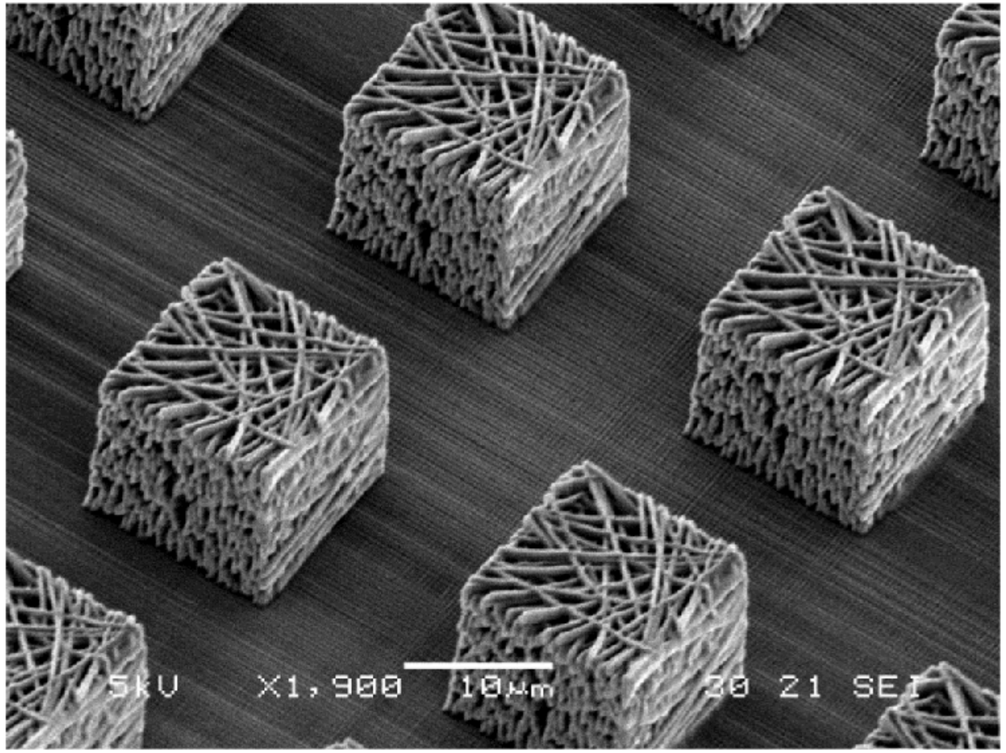
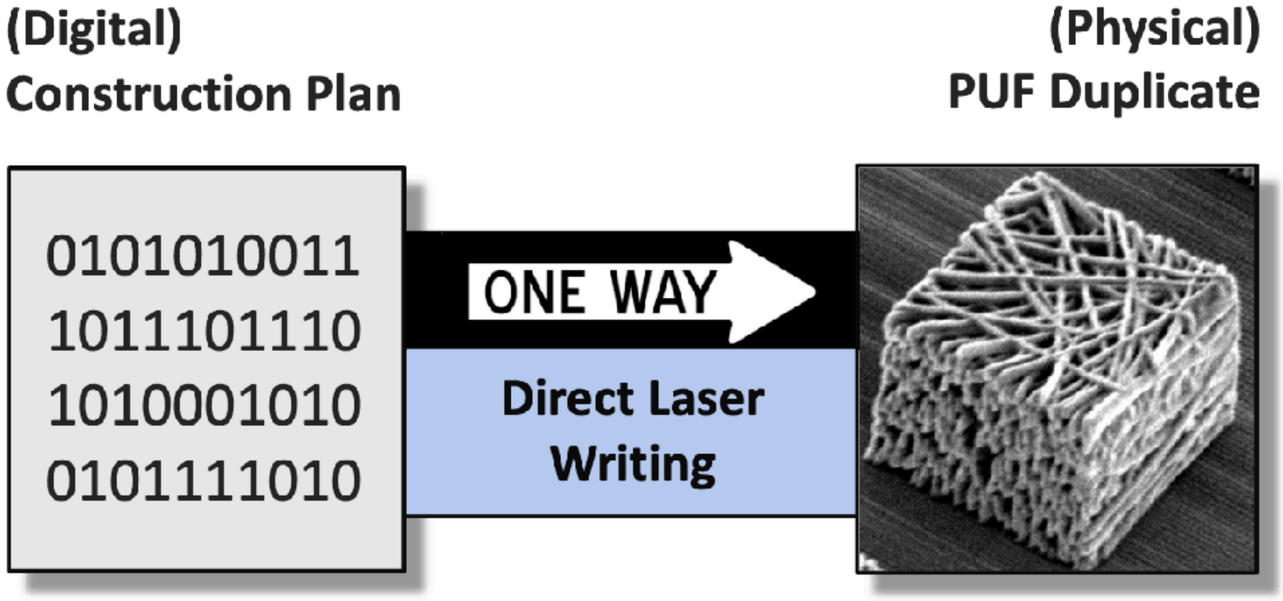
Physical Unclonable Functions

The first fifty years

Ravi Pappu / ASHES 2023

~ 1 year ago

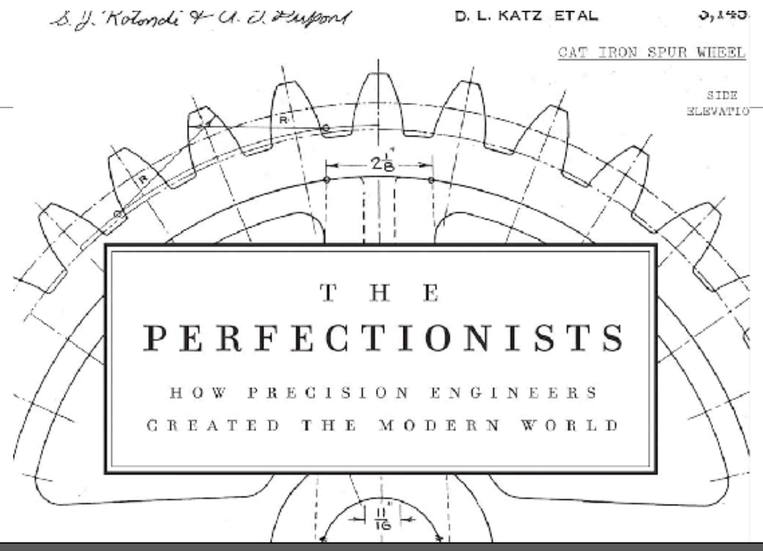




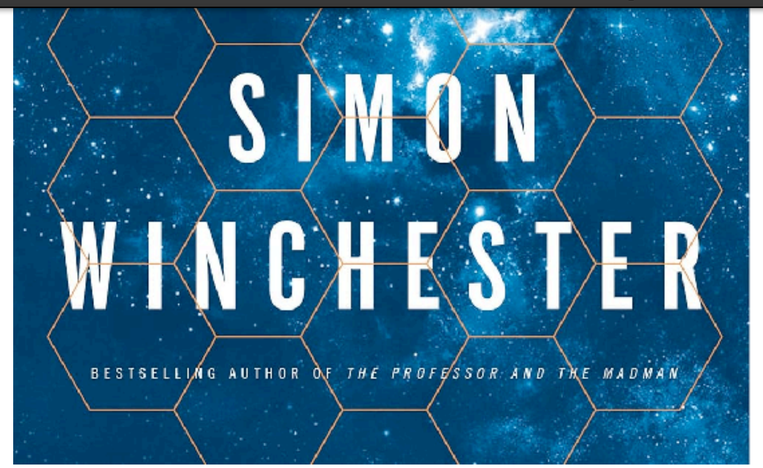
Marakis, E., Rührmair, U., Lachner, M., Uppu, R., Škorić, B., Pinkse, P.W.H., 2022. Clones of the Unclonable: Nanoduplicating Optical PUFs and Applications.

Today's talk

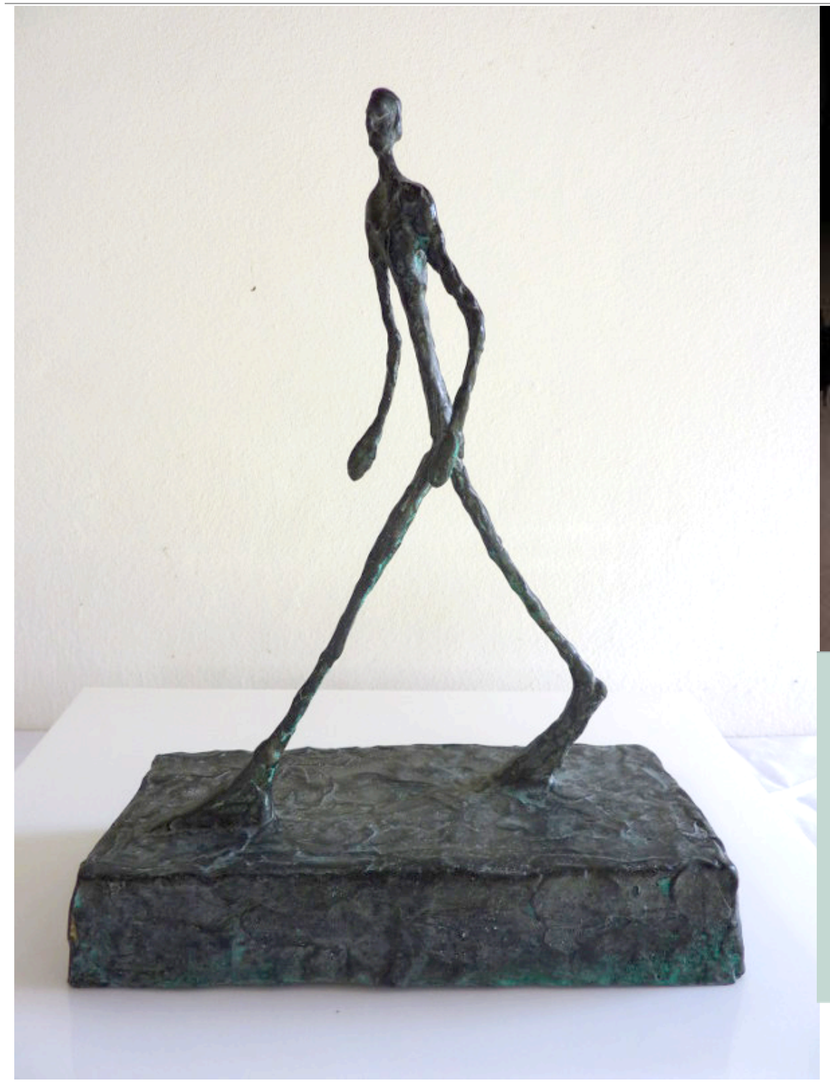
- A series of (un)fortunate events
- Towards a theory of unclonability
  - via points of interest in the PUF landscape



Precision must be duplicable.



Except, perhaps, in the art forgery world



"Long, thin figures, and an amorphous, crumbly surface," says Driessen. "It isn't difficult to make Giacomettis." After a while, he says, he "literally had Giacometti in my fingers." According to Driessen, it took him 30 to 40 minutes for the small figures. But they weren't simply recast versions of the originals. Instead, Driessen just added to Giacometti's body of work. He made his own models, had them cast and stamped them with the stamps of the foundries Giacometti had used.

Sontheimer, M. (2013) 'Art Forger Robert Driessen Reveals How He Made Giacometti Fakes', *Der Spiegel*, 10 April.

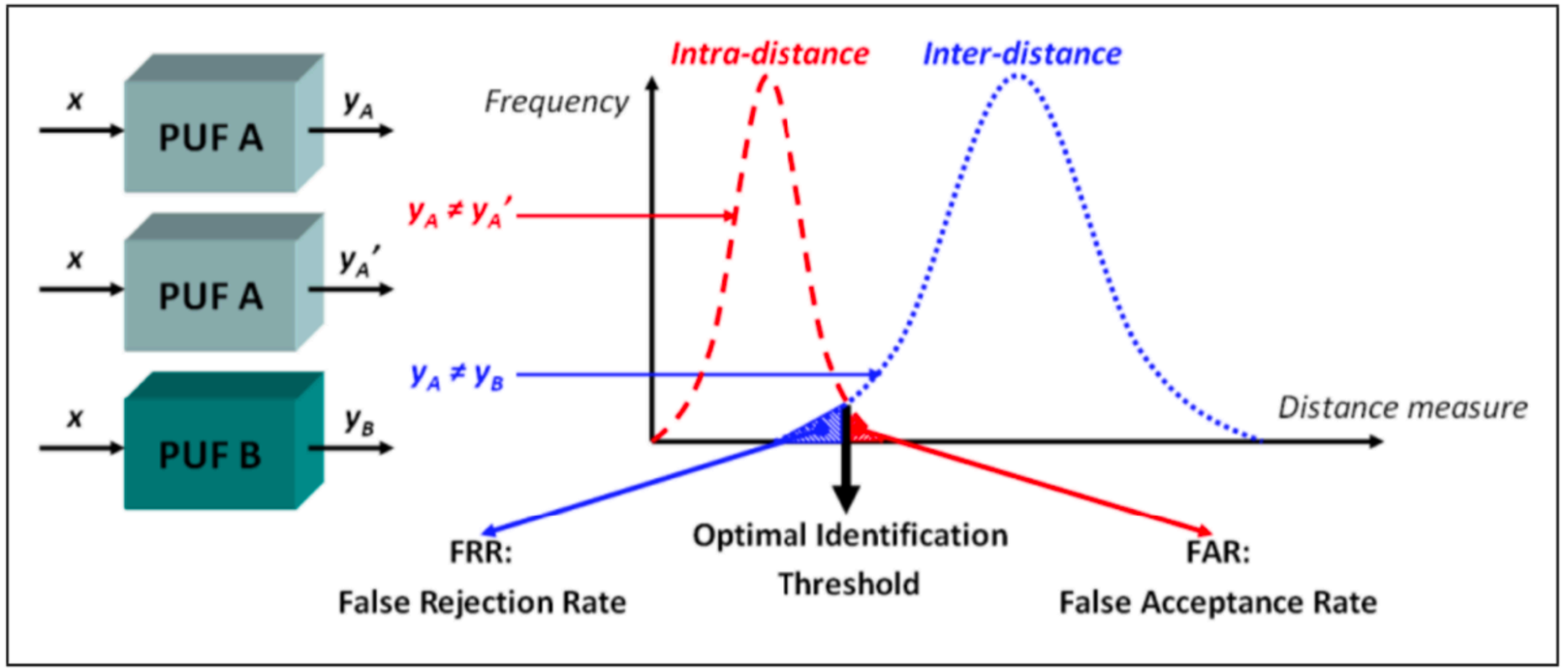
One-page handbook of PUFs

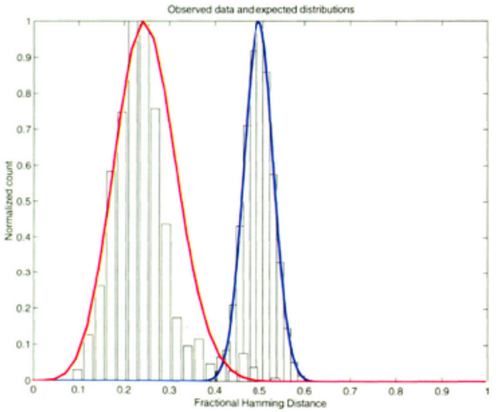
- A PUF comprises
  - A physically disordered structure *S* i.e., frozen randomness
  - A set of challenges against *S* and corresponding responses {*C,R*} aka. CRPs
  - Challenges are physically-based probes that interact with structure
  - This interaction extracts some of the frozen randomness from the structure
  - Responses to challenges are “computed” rapidly by physics, but are “hard” to predict or model.

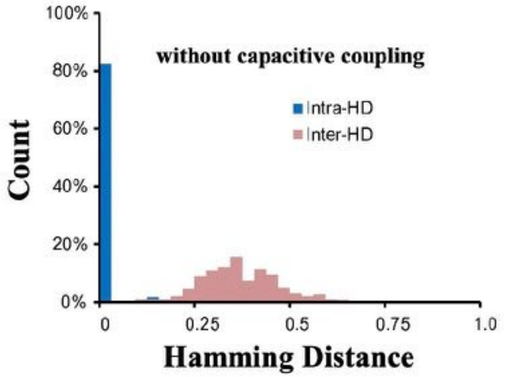
- Key properties
  - *Reproducibility*: For a given structure, the same challenge generates the same (noisy) response
  - *Uniqueness*: The same challenge generates different responses for different structures
  - *Reliability*: These properties are stable over time

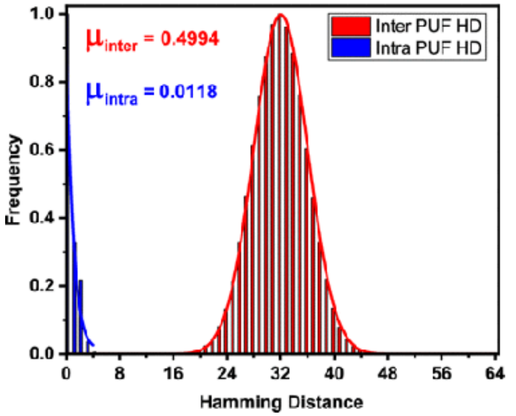
- Weak vs. Strong PUFs
  - Distinguished by the cardinality of {*C*} or {*R*}

Inter/Intra-PUF Hamming Distance Distributions



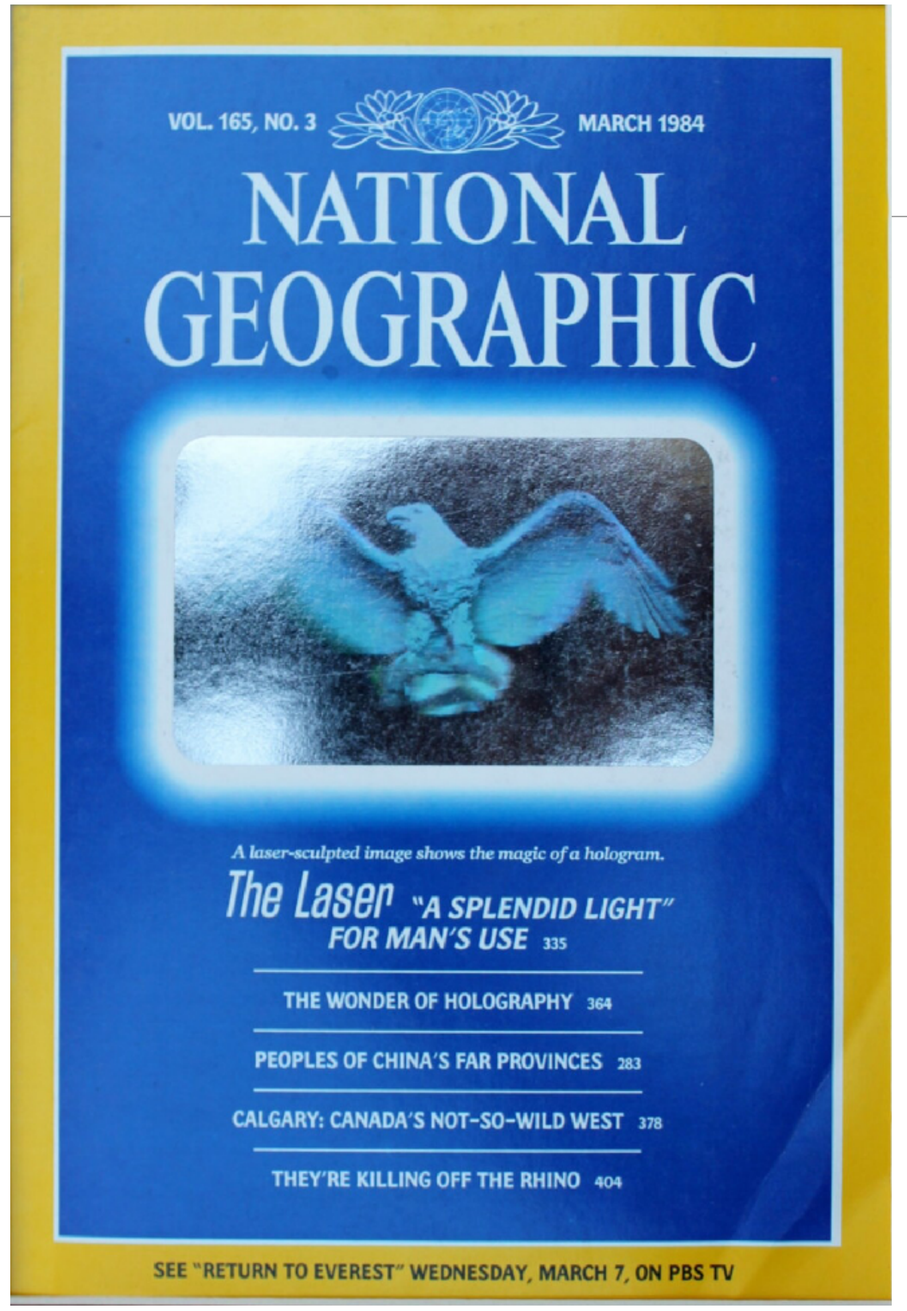






Maes, R. *et al*. in *Towards Hardware-Intrinsic Security* (eds. Sadeghi, A.-R. et al.) 3–37 (Springer Berlin Heidelberg, 2010)

1984


VOL. 165, NO. 3
MARCH 1984
NATIONAL GEOGRAPHIC
A laser-sculpted image shows the magic of a hologram.
The Laser "A SPLENDID LIGHT" FOR MAN'S USE 335
THE WONDER OF HOLOGRAPHY 364
PEOPLES OF CHINA'S FAR PROVINCES 283
CALGARY: CANADA'S NOT-SO-WILD WEST 378
THEY'RE KILLING OFF THE RHINO 404
SEE "RETURN TO EVEREST" WEDNESDAY, MARCH 7, ON PBS TV

1989

The Media Laboratory

Massachusetts Institute
of Technology
20 Ames Street
Cambridge, Massachusetts
02139

August 24, 1989

Ravikanth Srinivasa Pappu
C-22 Shanti Shikara,
Somajiguda, Hyderabad - 500 482.
AP, India

Dear Mr. Pappu,

Thank you for your note of July 18. I'm sorry to hear that your plans to pursue a holographic television system project did not work out for this year. You have asked me to suggest a problem that you might work on for your project, and I'm happy to offer what I can.

I expect that the most interesting direction of holography for you to pursue will be the connection between computers and holograms, and it may be possible to pursue a simple holographic stereogram system in the time you have remaining. I am enclosing a reprint that surveys some of the literature of holographic stereograms, and I hope that will help you get started. There will still be a certain amount of hardware to gather, but I think you will find the results interesting enough to warrant that effort.

Best of luck with whatever project you choose to pursue.

Very truly yours,

Stephen A. Benton
Professor of Media Technology
Director, Spatial Imaging Group

1993

Holographic TV
MIT

1998 - Holographic Video + Haptics

Plesniak, W., Pappu, R. and Benton, S. (2003) ‘Haptic holography: A primitive computational plastic’, *Proceedings of the IEEE*, 91(9), pp. 1443–1456.

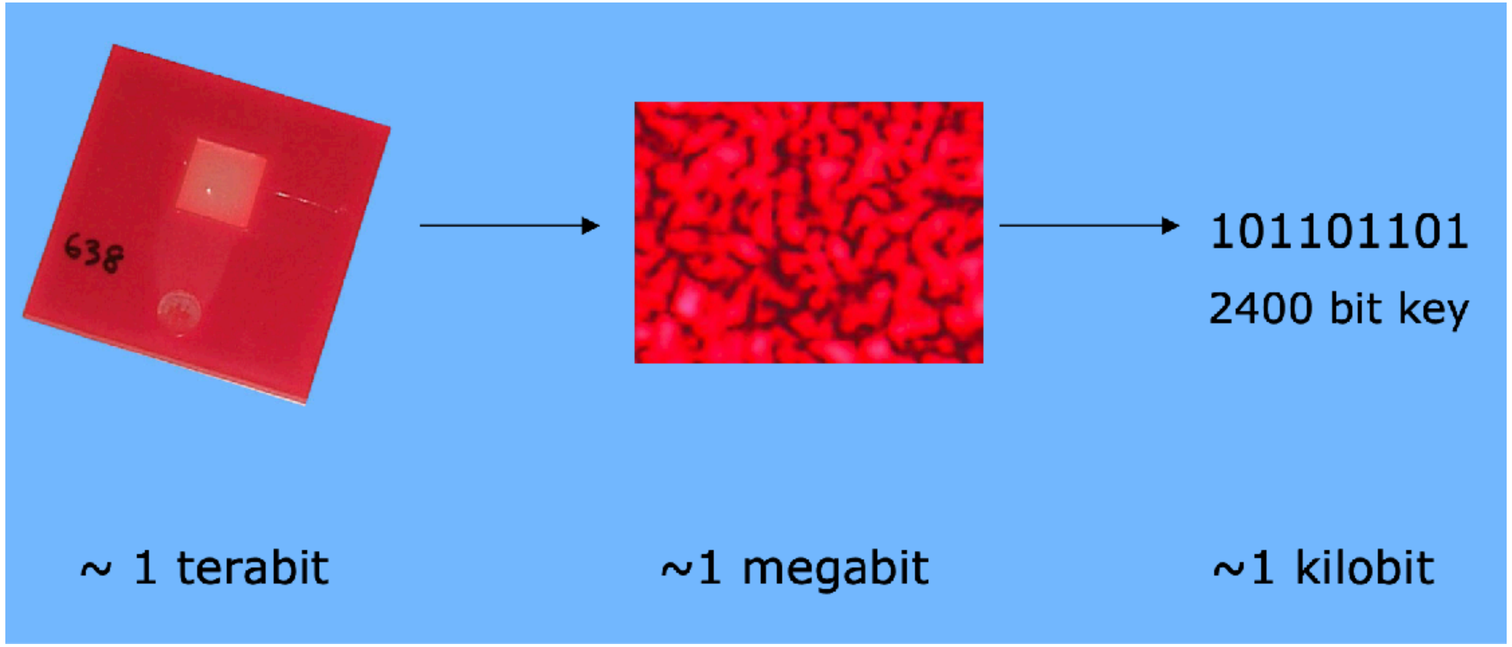
1997 - 1999: Fighting speckle

Introduction

Laser speckle noise is a direct consequence of the high coherence of laser light and has been long recognized as the Enemy Number One of holography. When a hologram is taken of a transparency illuminated with a single plane or spherical wave nothing is lost of the information content. The resolution is given by the angle subtended by the hologram as seen from the object. But the reconstructed image of the object is marred by the schlieren of the optical system; every speck of lens cement, every particle of dust shows up as a system of interference fringes. Only lensless Fourier holograms are

Gabor, D., 1970. Laser Speckle and Its Elimination. IBM J. Res. & Dev. 14, 509–514.

1999 - Physical One-Way Functions



What’s in a name?

Physical One-Way Hash Functions

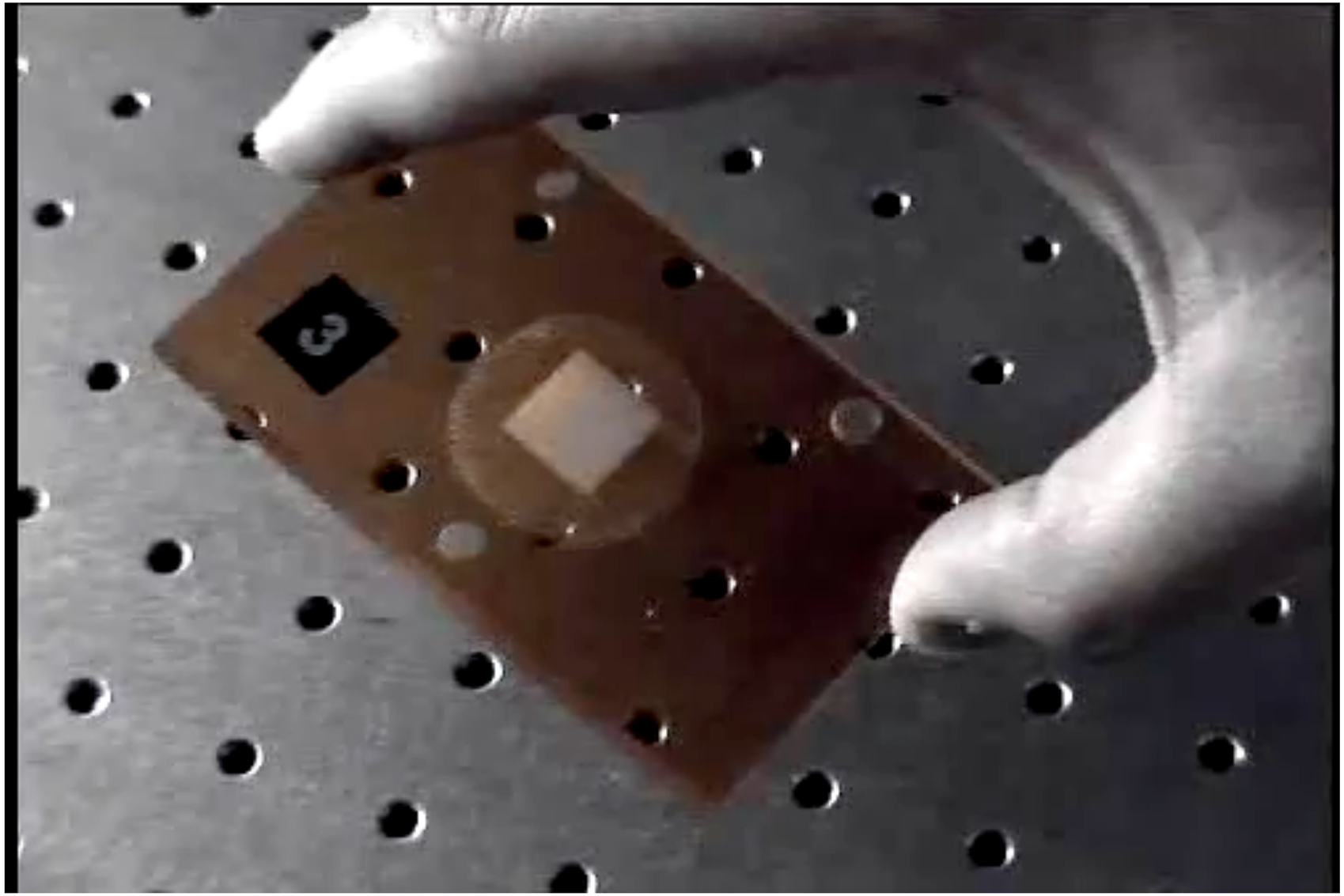
Physical One-Way Functions

Physical Random Oracles

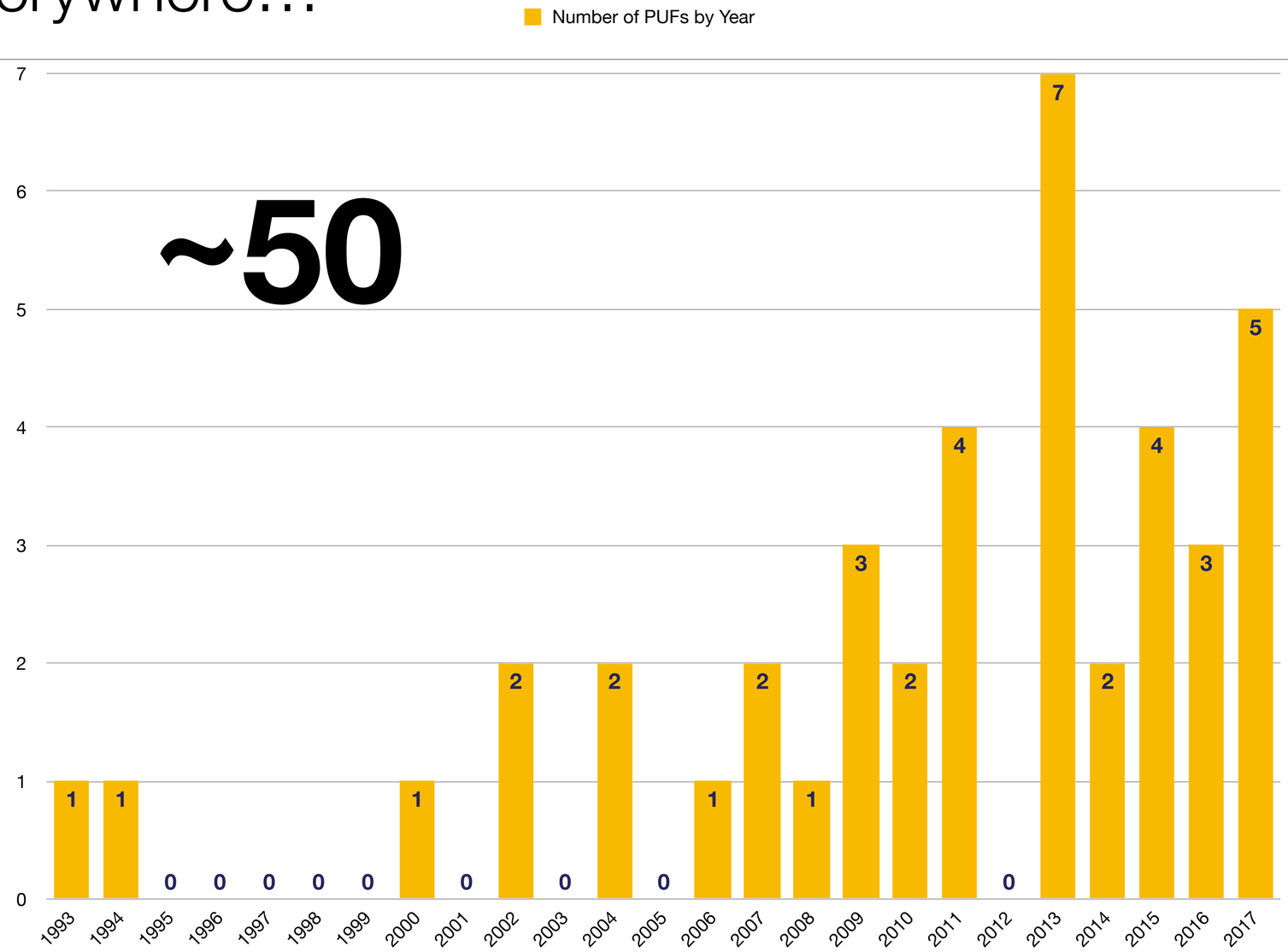
Physical Random Functions

Physical Unclonable Functions

1999 - Physical One-Way Functions

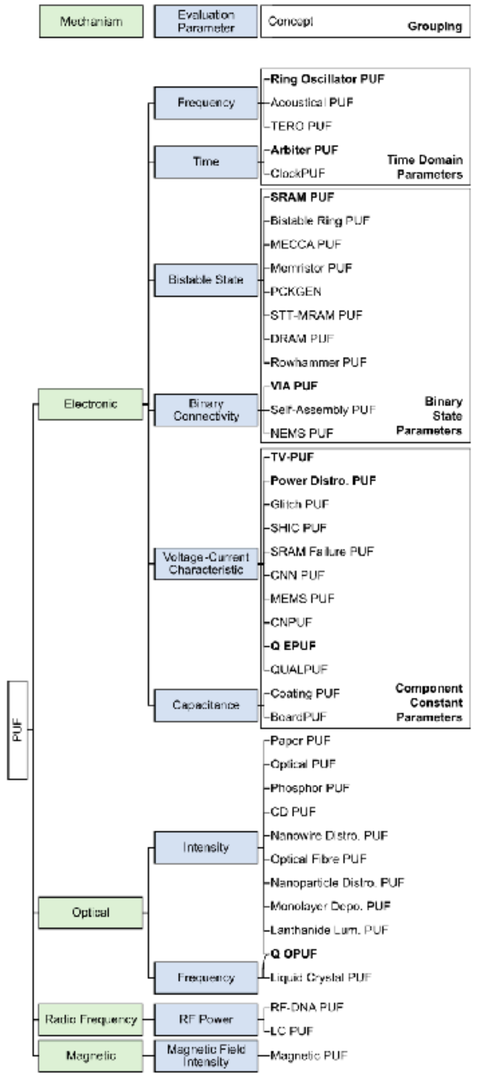


PUFs are everywhere…

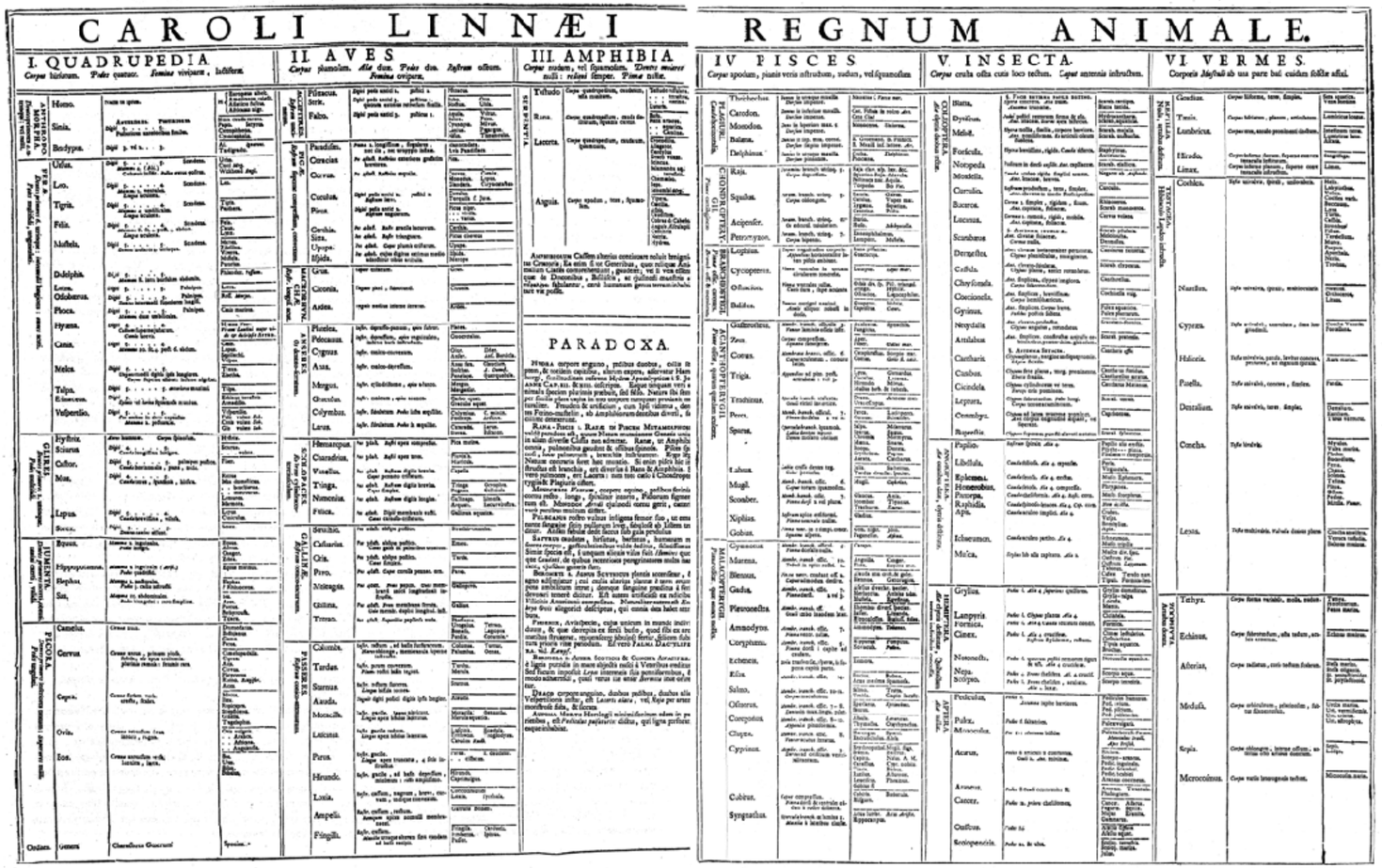


McGrath, T. *et al*. *Applied Physics Reviews* 6, 011303 (2019)

…but developing a taxonomy is hard



McGrath, T. *et al*. *Applied Physics Reviews* 6, 011303 (2019)



https://en.wikipedia.org/wiki/Linnaean_taxonomy

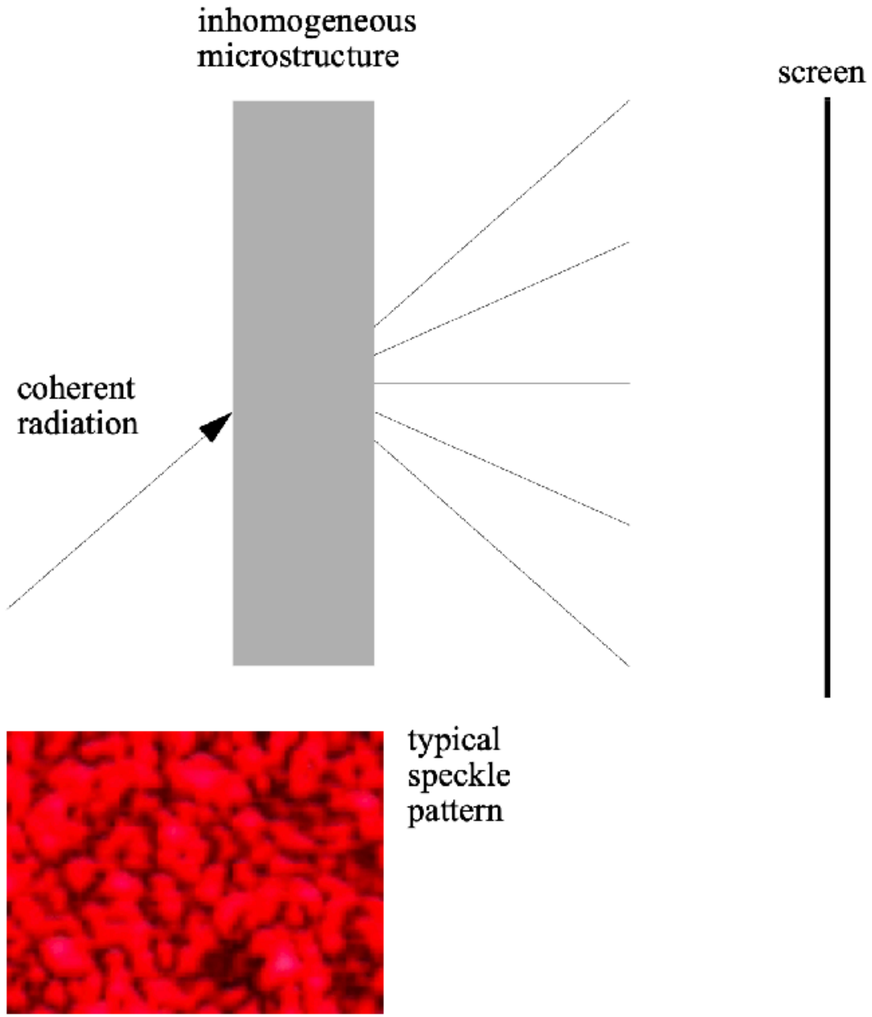
Towards a Theory Of Unclonability

1. Where do strong PUFs come from?
2. How do we characterize strong PUFs?
3. Like computability classes, can we conceive of unclonability classes?
   - Is it harder to clone strong PUFs than weak PUFs? *Fabrication Complexity*.
   - If a strong PUF is harder to model, is it also harder to clone?

> *"Practically, cloning can be very hard or infeasible. Demonstrating theoretical unclonability on the other hand is very difficult. The only known systems which can be proven to be theoretically unclonable are based on quantum physics."*

Maes, R. et al. in Towards Hardware-Intrinsic Security (eds. Sadeghi, A.-R. et al.) 3–37 (Springer Berlin Heidelberg, 2010)

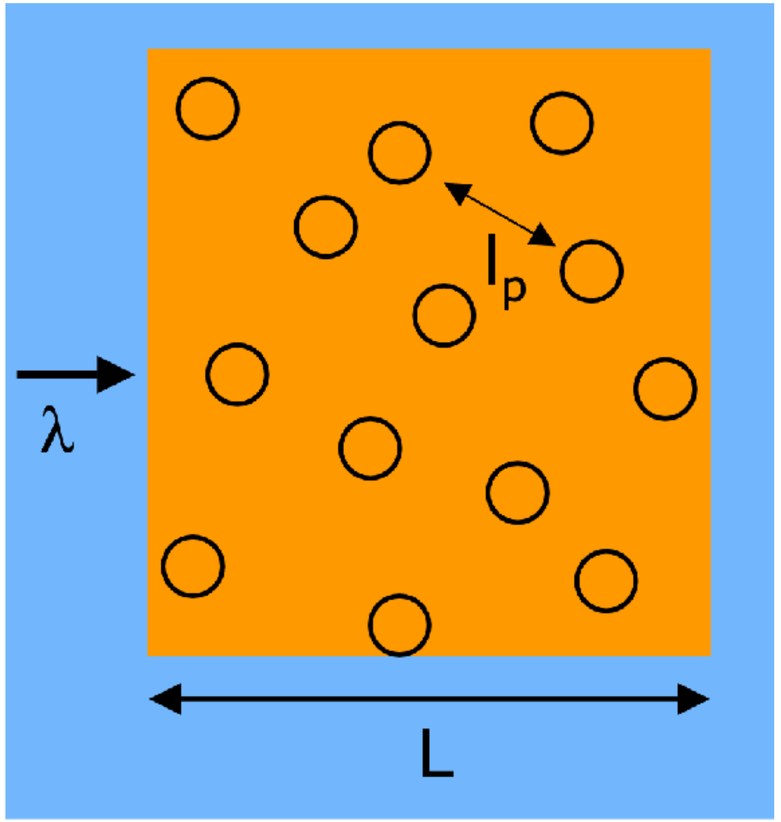
What is the DNA of an optical strong PUF?



Temporal Coherence

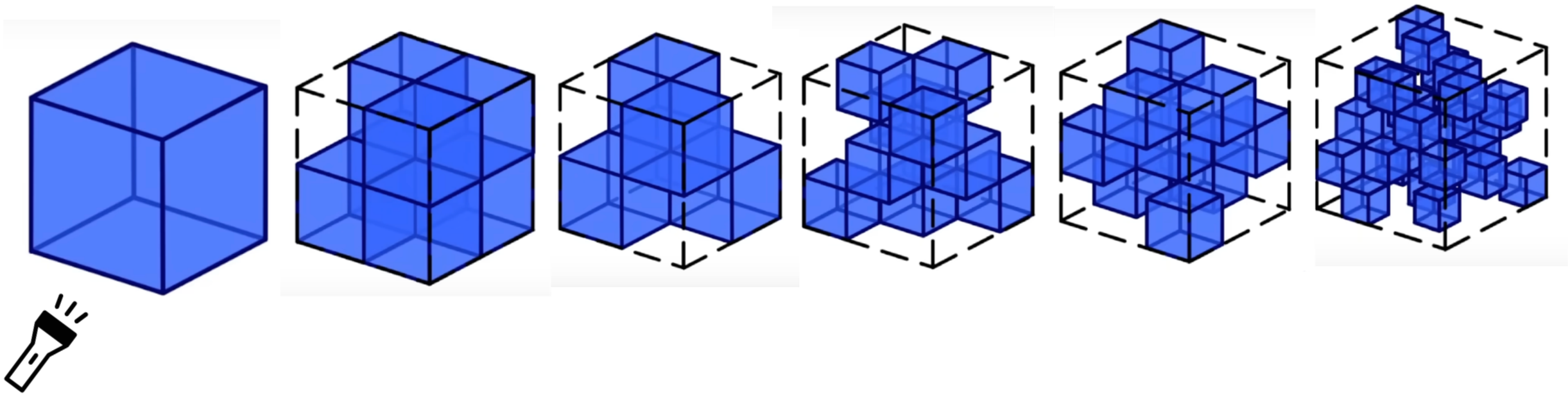
- Output phase *remembers* previous interactions with each scatterer
- *Accumulates* information about the inhomogeneity
- Enables *interference*, not just addition of intensities

I think it is possible to generalize this concept of temporal coherence to other PUF types

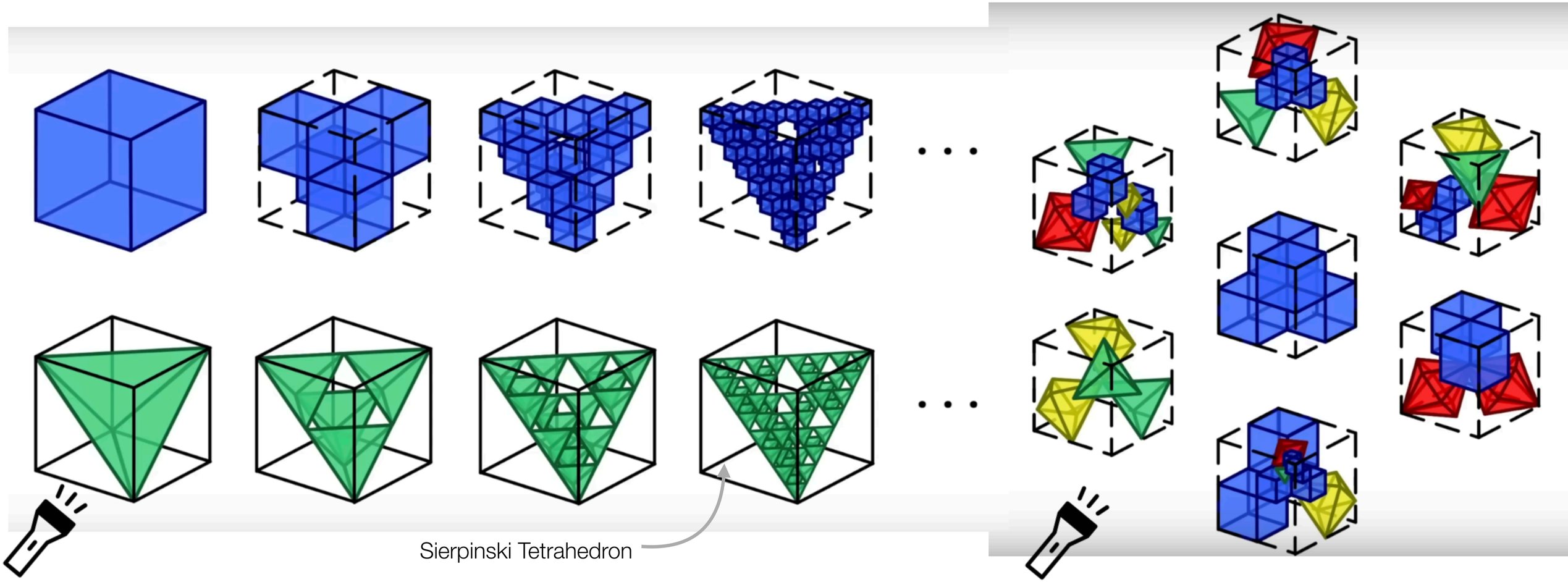


Imagine if the illumination were incoherent

- You'll simply get a shadow plus scattered light.



Infinite structural complexity with identical output



Can You Guess a Shape from Its Shadows?, dir. by Ben Gobler, 2023 <https://www.youtube.com/watch?v=Cnhr6VaQK1g> [accessed 24 November 2023]

Temporal coherence as a physical resource

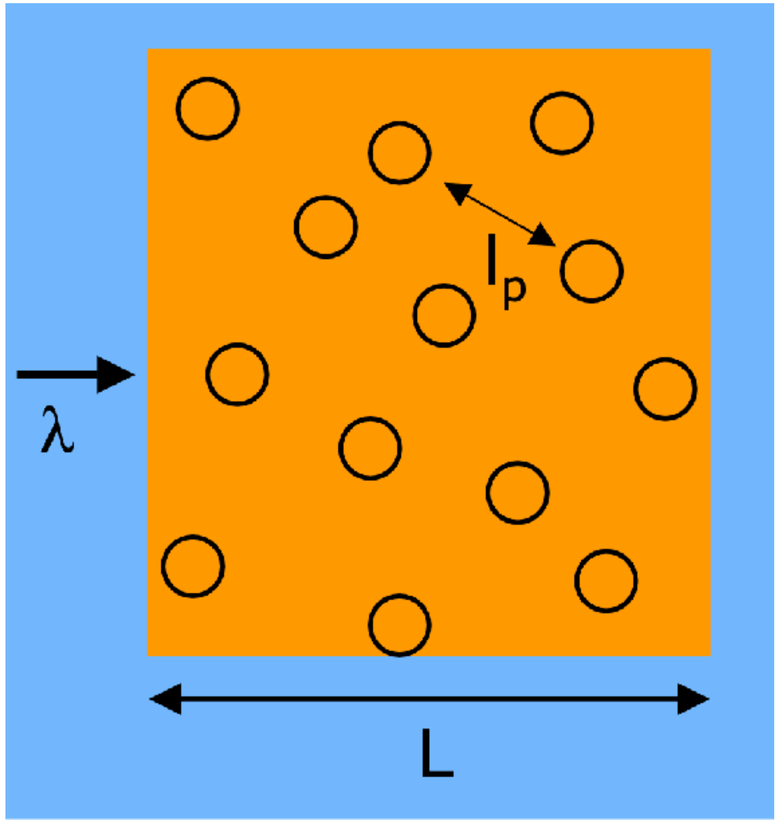
Shadows — Speckle

Incoherent — Partially Coherent — Coherent

Spatial Utilization

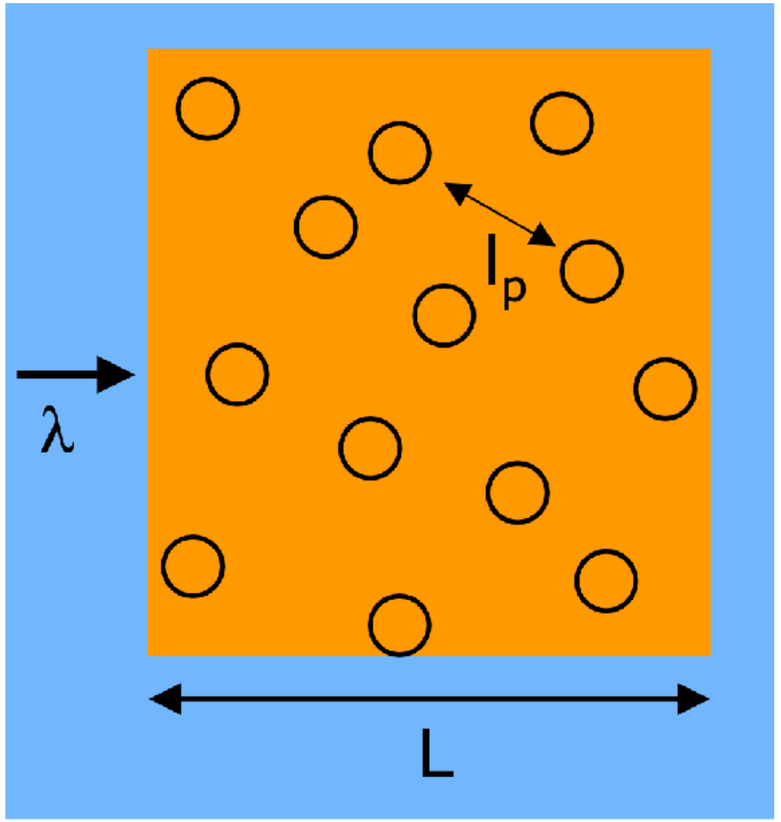
- *More* of the structure is involved
- *Many* scatterers (i.e., interactions) per path
- *Multiple paths* per challenge

Temporal coherence and greater spatial utilization enable the combinatorial explosion of CRPs.

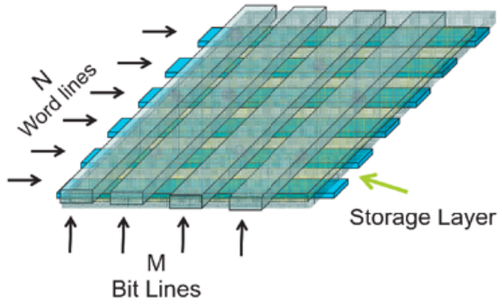


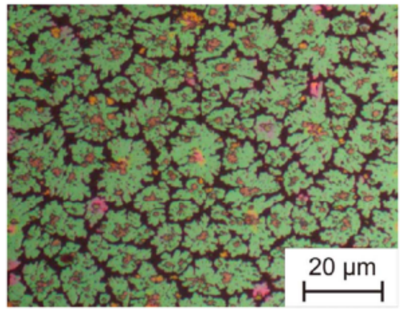
Reversibility

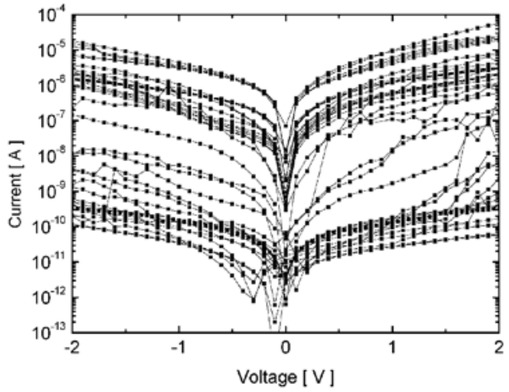
- Process is **reversible** in principle
  - No *erasure* or *level restoring* within the structure



SHIC PUFs based on crossbar arrays



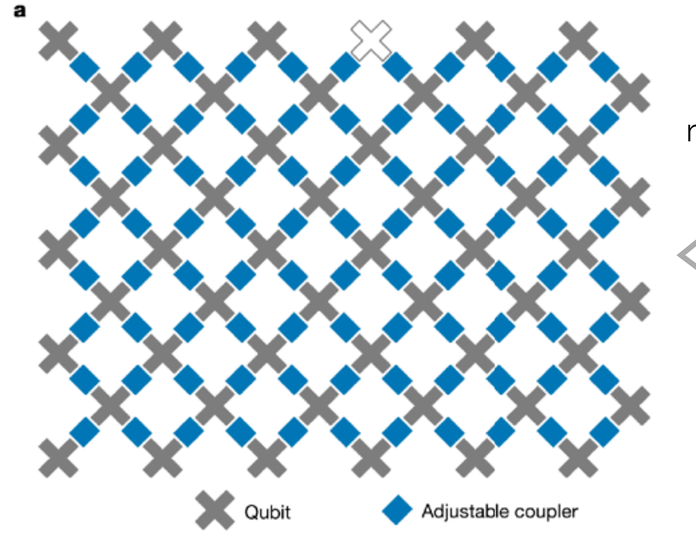




- Coherence: Resistance depends *history* of interaction along the lines
- Multiple interactions with randomness along any path
  - *Spatial utilization* depends on challenge and response location
- No erasure or level-restore

Rührmair, U. et al. (2011) 'Applications of High-Capacity Crossbar Memories in Cryptography', IEEE Transactions on Nanotechnology, 10(3), pp. 489–498.

Google's quantum computer is a provably strong PUF



"Sampling the quantum circuit's output produces a set of bitstrings, for example {0000101, 1011100, ...}. Owing to quantum interference, the probability distribution of the bitstrings ***resembles a speckled intensity pattern produced by light interference in laser scatter****, such that some bitstrings are much more likely to occur than others. Classically computing this probability distribution becomes exponentially more difficult as the number of qubits (width) and number of gate cycles (depth) grow."*

"Note that our protocol's output is unpredictable even to a computationally unbounded adversary who can see the random oracle."

Aaronson, S. and Hung, S.-H. (2023) 'Certified Randomness from Quantum Supremacy',

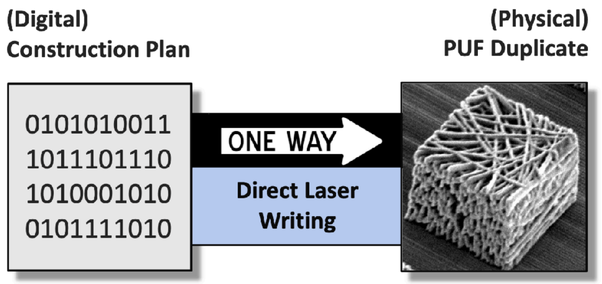
Arute, F. et al. (2019) 'Quantum supremacy using a programmable superconducting processor', Nature, 574(7779), pp. 505–510.

Conjecture

Generalized temporal coherence and high spatial utilization are necessary conditions for strong PUFs.

How to characterize PUFs?

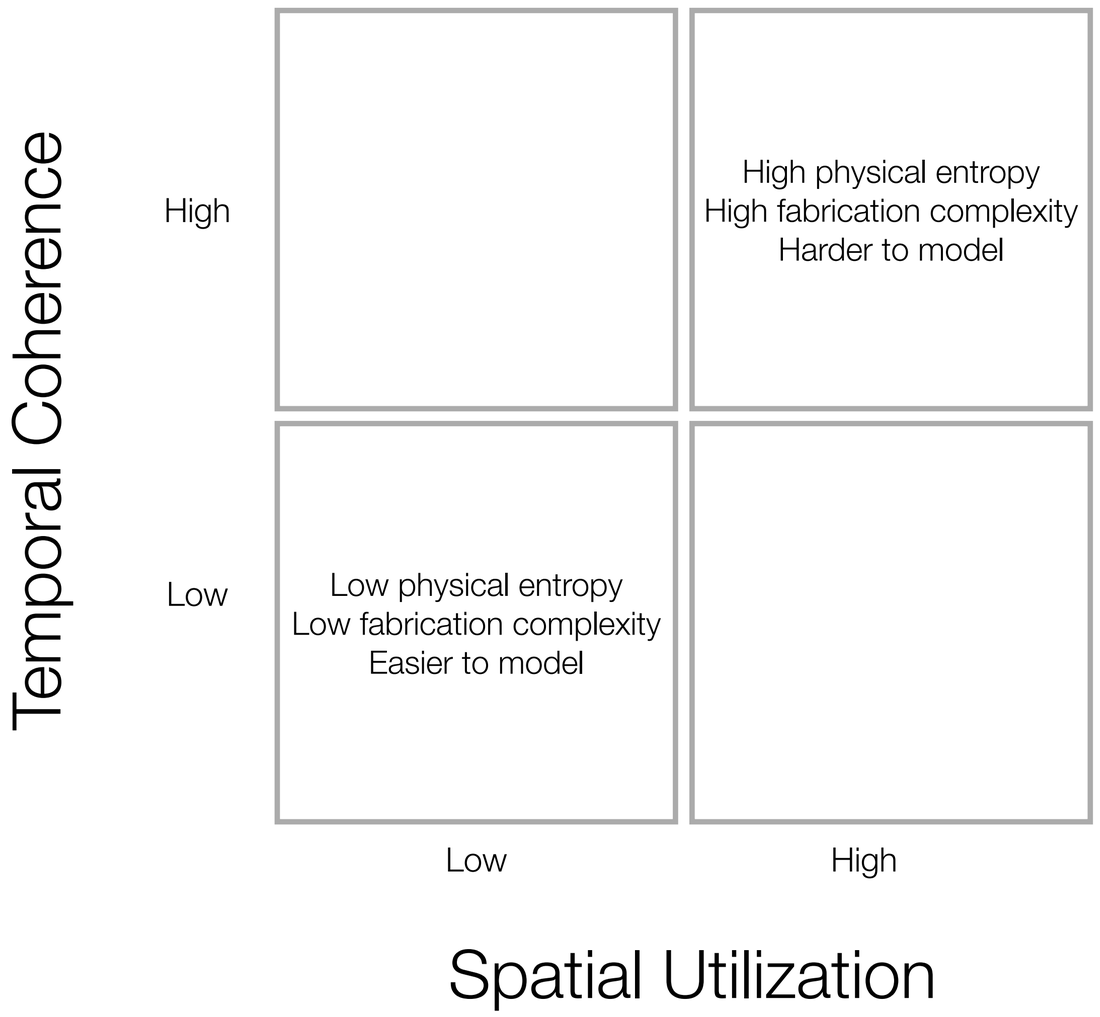
- Need to characterize both structural and Shannon information.
- Zurek has proposed using the sum of
  - Kolmogorov complexity (or Algorithmic Randomness) for the structure
  - Shannon entropy for the output
- *Physical Entropy*



+ ~10^{70} bits

Zurek, W.H. (1989) 'Algorithmic randomness and physical entropy', *Physical Review A*, 40(8), pp. 4731–4751. Available at: https://doi.org/10.1103/PhysRevA.40.4731.

Unclonability Classes Conjecture



Looking ahead…

In the next decade, we'll be able to "sequence" a structure and estimate properties like coherence, spatial utilization, physical entropy, and the difficulty of cloning.

Of course, it would be great to actually clone a strong PUF!