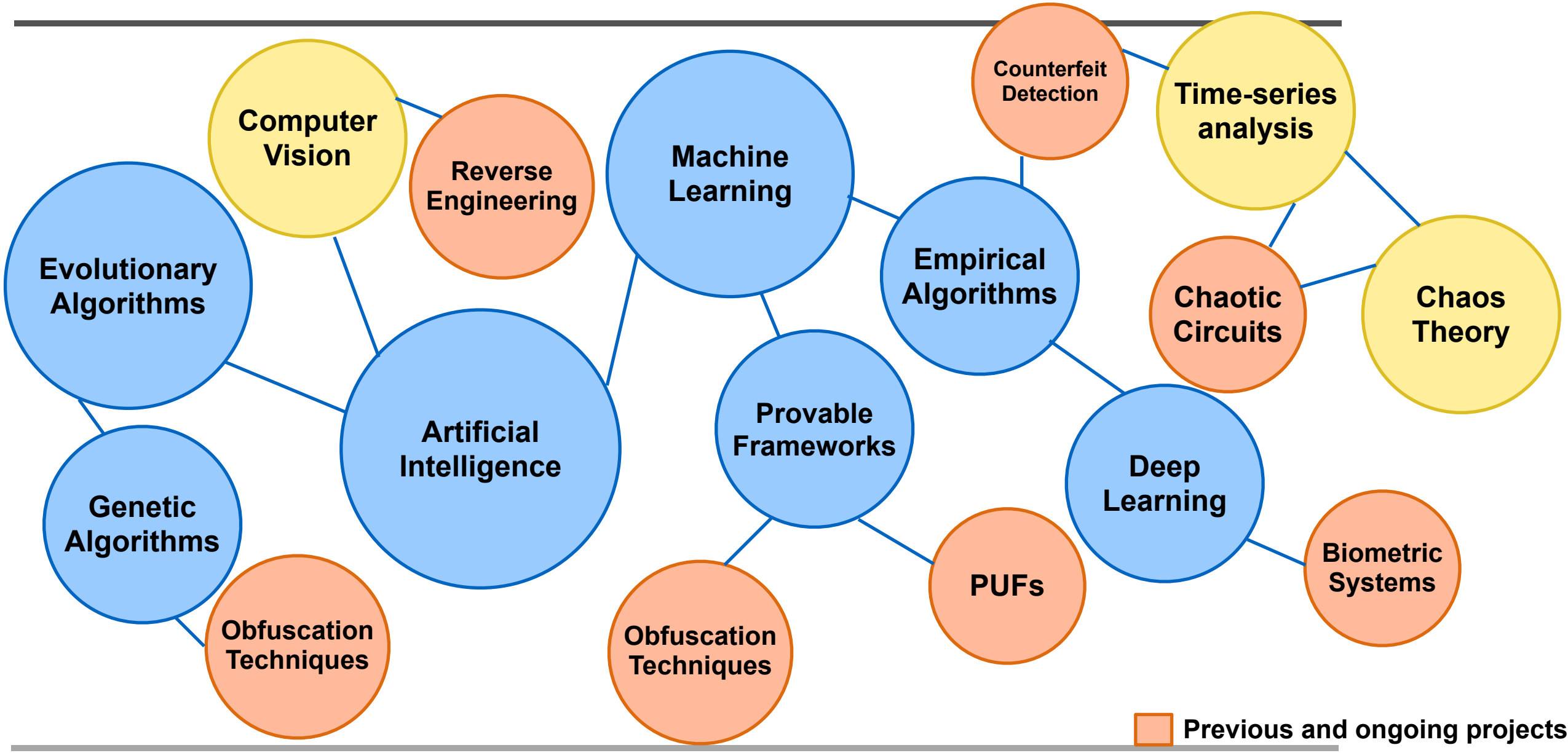
WPI

From Cryptography to Property Testing

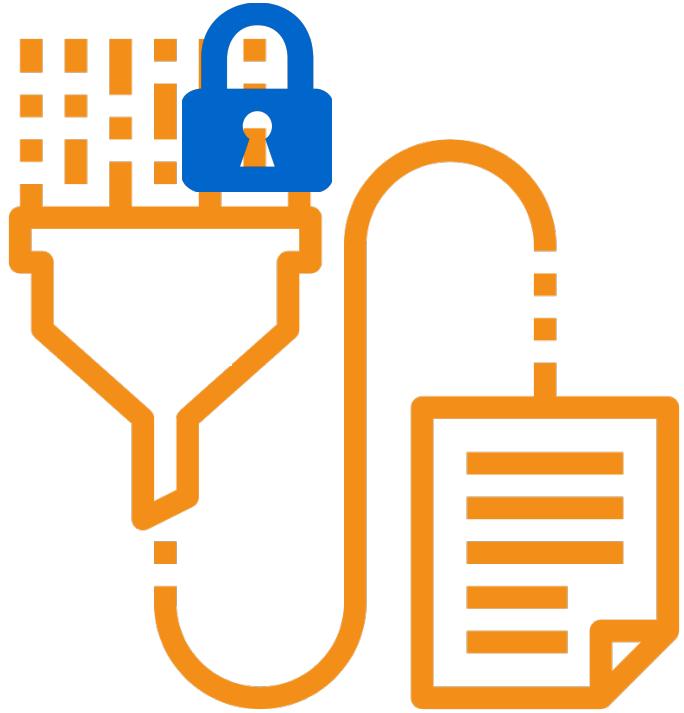
Fatemeh (Saba) Ganji, Ph.D.


Computer Vision
Reverse Engineering
Machine Learning
Counterfeit Detection
Time-series analysis
Evolutionary Algorithms
Empirical Algorithms
Chaotic Circuits
Chaos Theory
Artificial Intelligence
Provable Frameworks
Deep Learning
Genetic Algorithms
Obfuscation Techniques
Obfuscation Techniques
PUFs
Biometric Systems
Previous and ongoing projects

Machine Learning and Cryptanalysis

Sister fields: machine learning and cryptanalysis

- **Sharing several notions and concerns [1]**
  - **Cryptanalysis: “breaking” some cryptosystem to find the secret key using typically, a large quantity of matching ciphertext and plaintext**
  - **The problem of “learning an unknown function” from examples of its input/output behavior, with prior knowledge about the class of possible functions**
- **Good cryptography can provide examples of classes of functions that are hard to learn [2].**



[1] Rivest, R.L., 1991, November. Cryptography and machine learning. In International Conference on the Theory and Application of Cryptology (pp. 427-439). Springer, Berlin, Heidelberg.
[2] Valiant, L.G., 1984. A theory of the learnable. Communications of the ACM, 27(11), pp.1134-1142.

RESEARCH CONTRIBUTIONS

Artificial Intelligence and Language Processing

David Waltz Editor

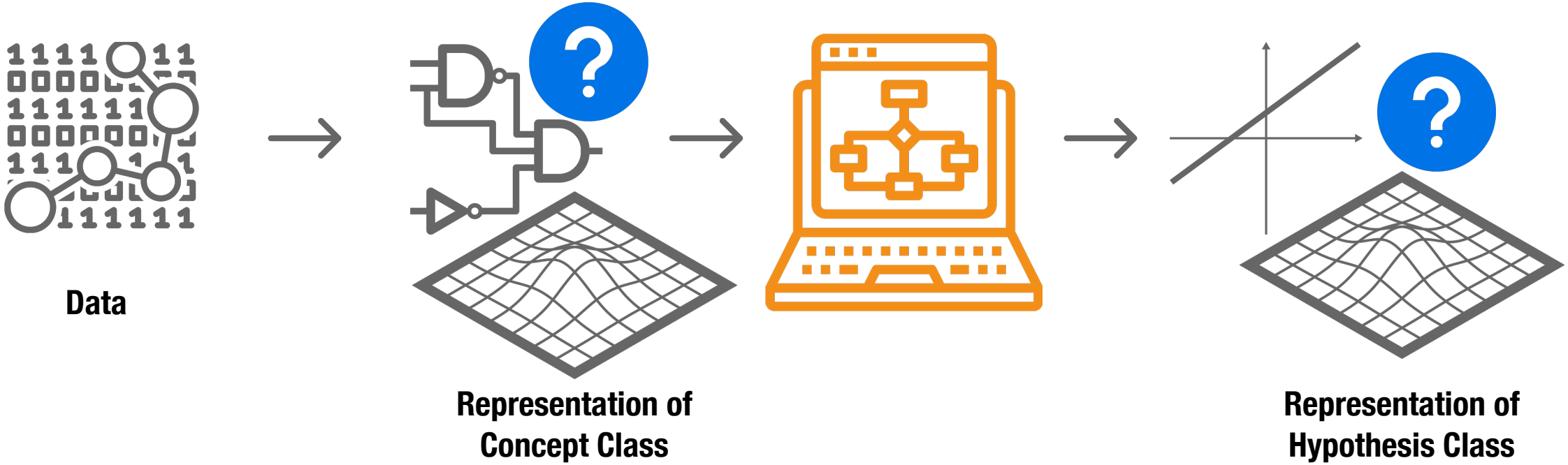
A Theory of the Learnable

L. G. VALIANT

ABSTRACT: *Humans appear to be able to learn new concepts without needing to be programmed explicitly in any conventional sense. In this paper we regard learning as the phenomenon of knowledge acquisition in the absence of explicit programming. We give a precise methodology for studying this phenomenon from a computational viewpoint.*

a genetically preprogrammed element, whereas some others consist of executing an explicit sequence of instructions that has been memorized. There remains a large area of skill acquisition where no such explicit programming is identifiable. It is this area that we describe here as learning. The recognition of familiar ob-

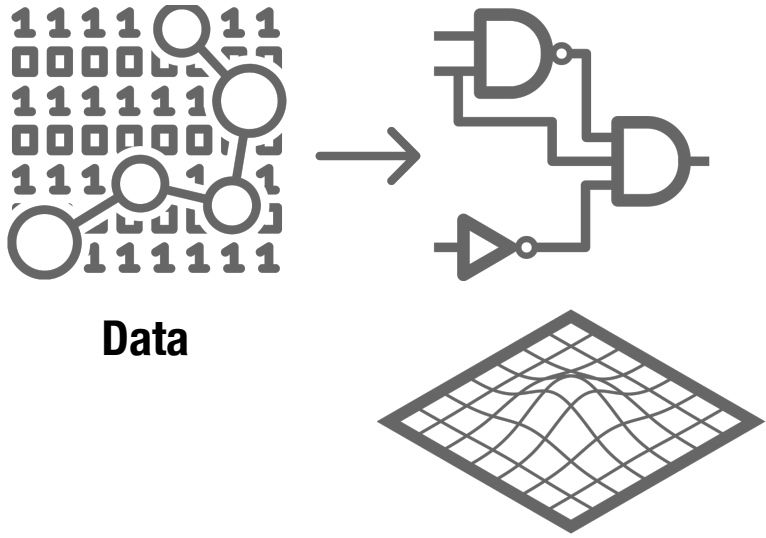
Steps taken in provable ML tasks



- Supervised learning, e.g., classification
- Probably Approximately Correct (PAC) learning approaches
  - Maximum number of examples for given levels of accuracy and confidence
  - Probability of delivering a desired model from the hypothesis class

Property testing

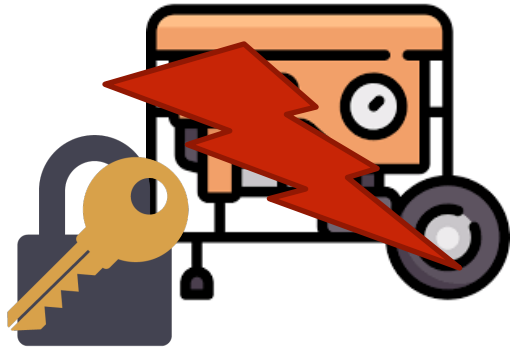
- How to choose the representation of concept class?
- Testing if a function has a pre-specified property [1]
  - Or significantly different from any through a distance measure
    - E.g., being linear or very far from that
  - Observing only a small sub-set of examples
  - A small failure probability for the algorithm
- Property testing vs. decision problems
  - Feasible approximation for an intractable problem
  - Approximate decision based on a limited number of examples
  - Efficient search due to the definition of distance measure



[1] Ron, D., 2008. Property testing: A learning theory perspective. Now Publishers Inc.

An Examples from Hardware Security

Why hardware security matters?



Secure key generation

Secure key storage

Secure execution

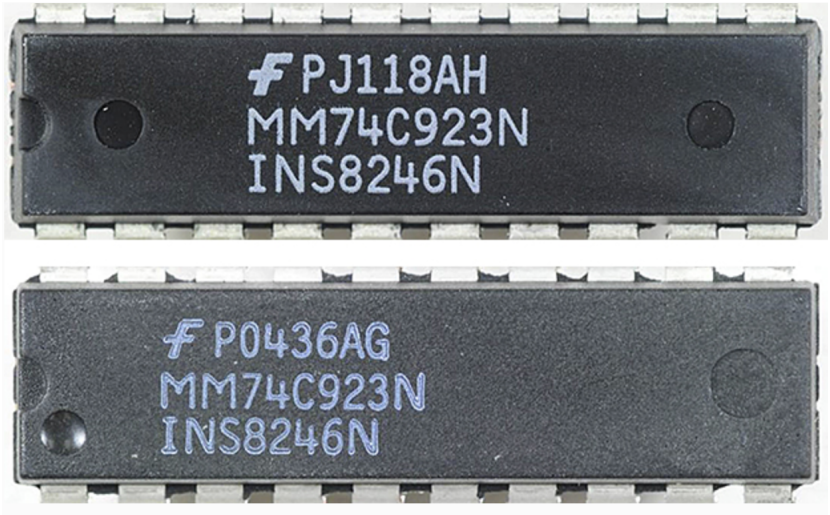
Example of Attacks:	**Insufficient randomness in a large collected set of public keys [1]**	**Difficult to stop adversaries from gaining physical access to key memories [2]**	**Break the security on the software and the hardware level [3]**

Physical Roots of Trust, e.g., PUFs, TRNGs, etc.

[1] Lim, D., Lee, J.W., Gassend, B., Suh, G.E., Van Dijk, M. and Devadas, S., 2005. Extracting secret keys from integrated circuits. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 13(10), pp.1200-1205.
[2] Torrance, R. and James, D., 2009, September. The state-of-the-art in IC reverse engineering. In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 363-381). Springer, Berlin, Heidelberg.
[3] Kocher, P., Jaffe, J. and Jun, B., 1999, August. Differential power analysis. In Annual International Cryptology Conference (pp. 388-397). Springer, Berlin, Heidelberg.

Physically Unclonable Functions (PUFs)

Motivation



Original

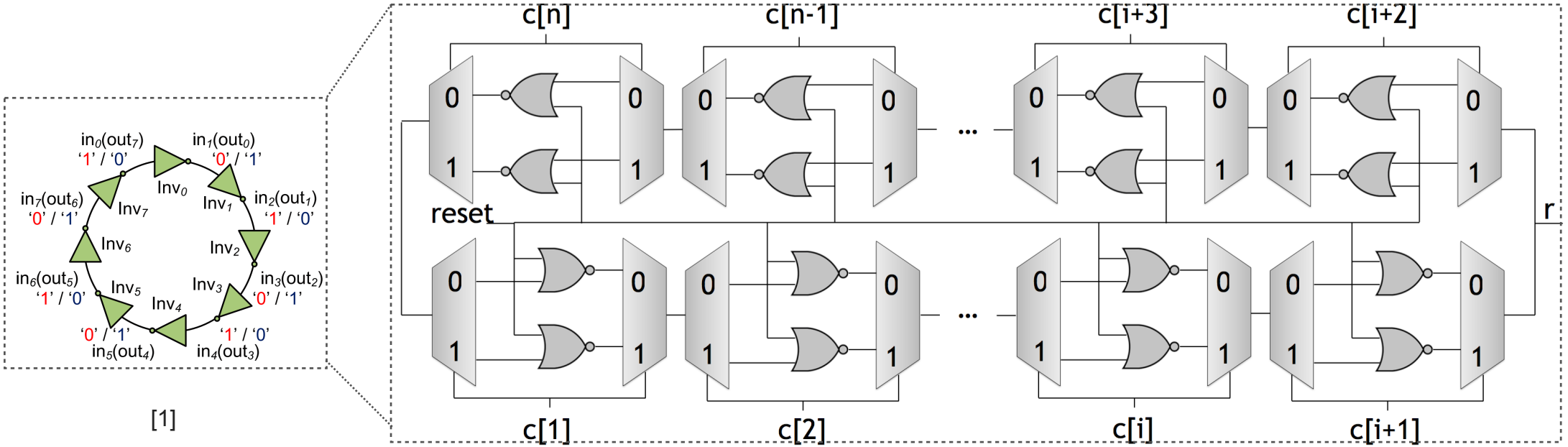
Photos: SMT Corp. [1]

- **Vulnerability of ICs to piracy and overbuilding attacks**
  - **According to the Semiconductor Industry Associates (SIA): it costs the US semiconductor companies billions in lost revenue [2].**
- **PUFs: Physically Unclonable Functions**

[1] Tehranipoor, M.M., Guin, U. and Bhunia, S., 2017. Invasion of the hardware snatchers. IEEE Spectrum, 54(5), pp.36-41.

[2] Koushanfar, F., Fazzari, S., McCants, C., Bryson, W., Sale, M., Song, P. and Potkonjak, M., 2012, June. Can EDA combat the rise of electronic counterfeiting?. In Proceedings of the 49th Annual Design Automation Conference (pp133-138). ACM.

Bistable Ring PUFs



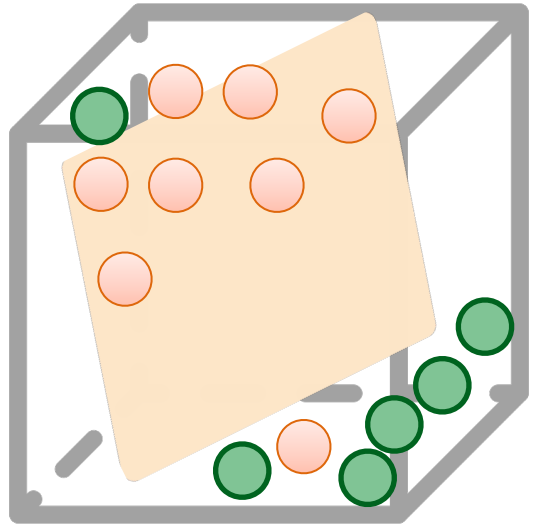
- **No precise mathematical model of the BR PUF functionality**
- **Linear threshold functions as representation of BR PUFs [1]**
  - **Simplified representation leading to the impossibility of increasing the learning accuracy arbitrarily**

[1] Chen, Q., Csaba, G., Lugli, P., Schlichtmann, U. and Rührmair, U., 2011, June. The bistable ring PUF: A new architecture for strong physical unclonable functions. In 2011 IEEE International Symposium on Hardware-Oriented Security and Trust (pp. 134-141). IEEE.
[2] Xu, X., Rührmair, U., Holcomb, D.E. and Burleson, W., 2015, June. Security evaluation and enhancement of bistable ring PUFs. In International Workshop on Radio Frequency Identification: Security and Privacy Issues (pp. 3-16). Springer, Cham.

Let's test it!

- **Methodology provided in [1] to test whether a Boolean-valued function is a halfspace (i.e., LTF)**
  - **Distinguishing between LTFs and functions being ε-far from any LTF**
  - **Only poly$(1/\varepsilon)$ examples: the minimum needed for learning is $\Omega(n/\varepsilon)$**
- **Experimental design**
  - **BR PUFs implemented on an Intel/Altera Cyclone IV FPGA, manufactured on a 60nm technology [2]**

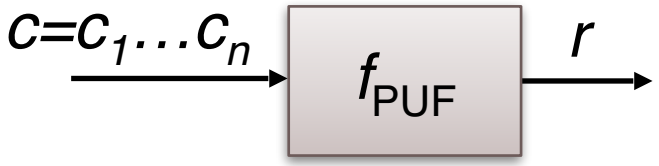
n	# CRPs	How far from any halfspace (min.) [%]
16	100	20
32	1339	40
64	63434	50



[1] Matulef, K., O'Donnell, R., Rubinfeld, R. and Servedio, R.A., 2010. Testing halfspaces. SIAM Journal on Computing, 39(5), pp.2004-2047.
[2] Ganji, F., Amir, S., Tajik, S., Forte, D. and Seifert, J.P., 2020, March. Pitfalls in machine learning-based adversary modeling for hardware systems. In 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE) (pp. 514-519). IEEE.

Let's test it against another class

- **k-junta testing: determining if the function f_{PUF} is in the class of k-junta functions**
  - **Determined by a small group of its input variables**
  - **Observation made by conducting experiments**



c	r
c=1…00	1
c'=1…11	1
c"=1…01	1

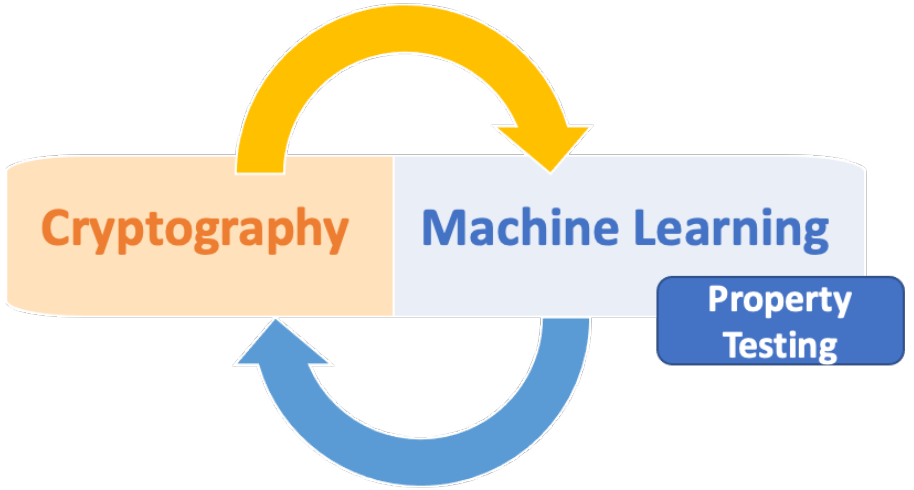
- **Test proposed in [1,2]: adaptive sampling, i.e., an example is drawn randomly, modified by flipping the variables, and then querying the function f_{PUF} on the these examples**
  - **Other tests available in [3]**

n	# CRPs	K
4	16	1
8	77	4
16	169	5
32	372	5
64	811	7

[1] Guijarro, D., Tarui, J. and Tsukiji, T., 1999, December. Finding relevant variables in PAC model with membership queries. In International Conference on Algorithmic Learning Theory (pp. 313-322). Springer, Berlin, Heidelberg.
[2] Ganji, F., Tajik, S., Fäßler, F. and Seifert, J.P., 2017. Having no mathematical model may not secure PUFs. Journal of Cryptographic Engineering, 7(2), pp.113-128.
[3] Ganji, F., Forte, D. and Seifert, J.P., 2019. PUFmeter a property testing tool for assessing the robustness of physically unclonable functions to machine learning attacks. IEEE Access, 7, pp.122513-122521.

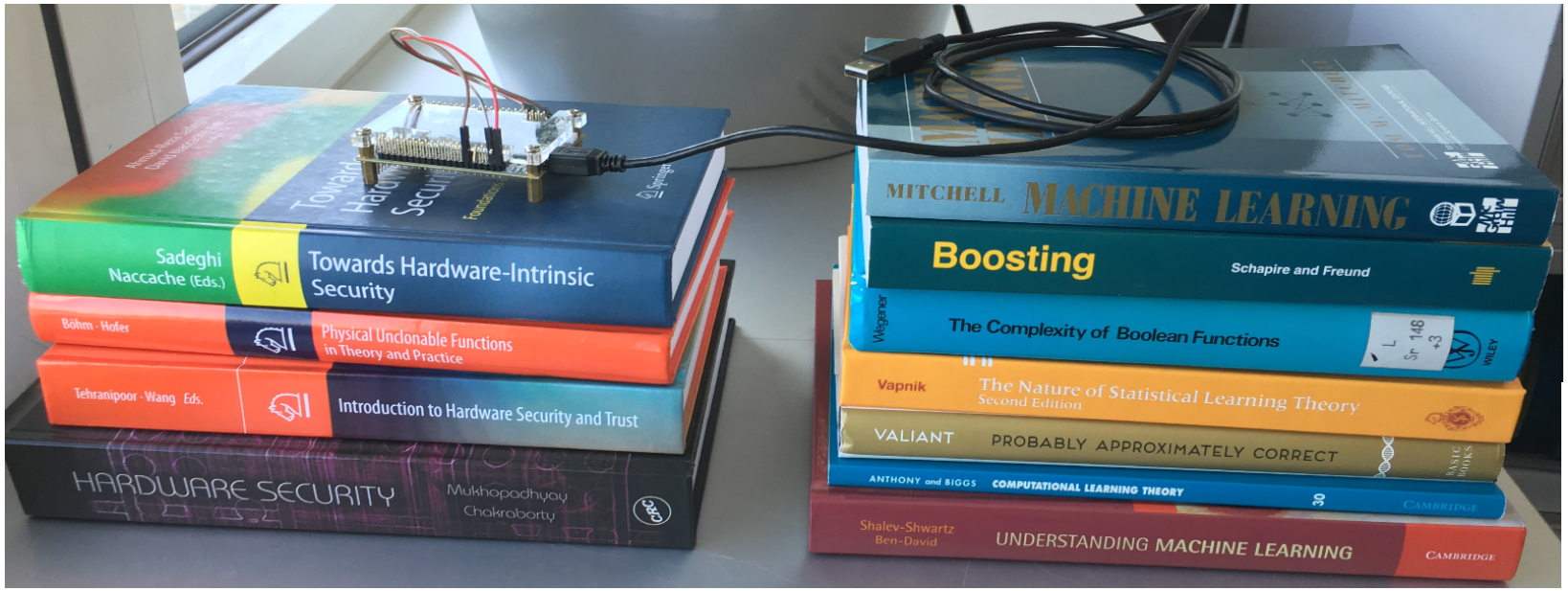
Take-home message

- What can be tested?
  - Algebraic properties, e.g., linearity
  - Boolean function classes, e.g., LTFs
- Which Boolean functions?
  - Experimental and/or simulation results
  - Closed-form mathematical model
- Important parameters and aspects
  - Distribution of the examples: distribution-free vs. uniformly chosen
  - Standard testing, tolerant testing, and distance approximation
  - Accept if ε_1-close to a function and reject if ε_2-far from that with $0 \leq \varepsilon_1 < \varepsilon_2 \leq 1$ (for standard test: ε_1=0)
  - Approximating the distance with a given error parameter δ [1]



[1] Guijarro, D., Tarui, J. and Tsukiji, T., 1999, December. Finding relevant variables in PAC model with membership queries. In International Conference on Algorithmic Learning Theory (pp. 313-322). Springer, Berlin, Heidelberg.

Thank you for your attention!



© Fatemeh Ganji