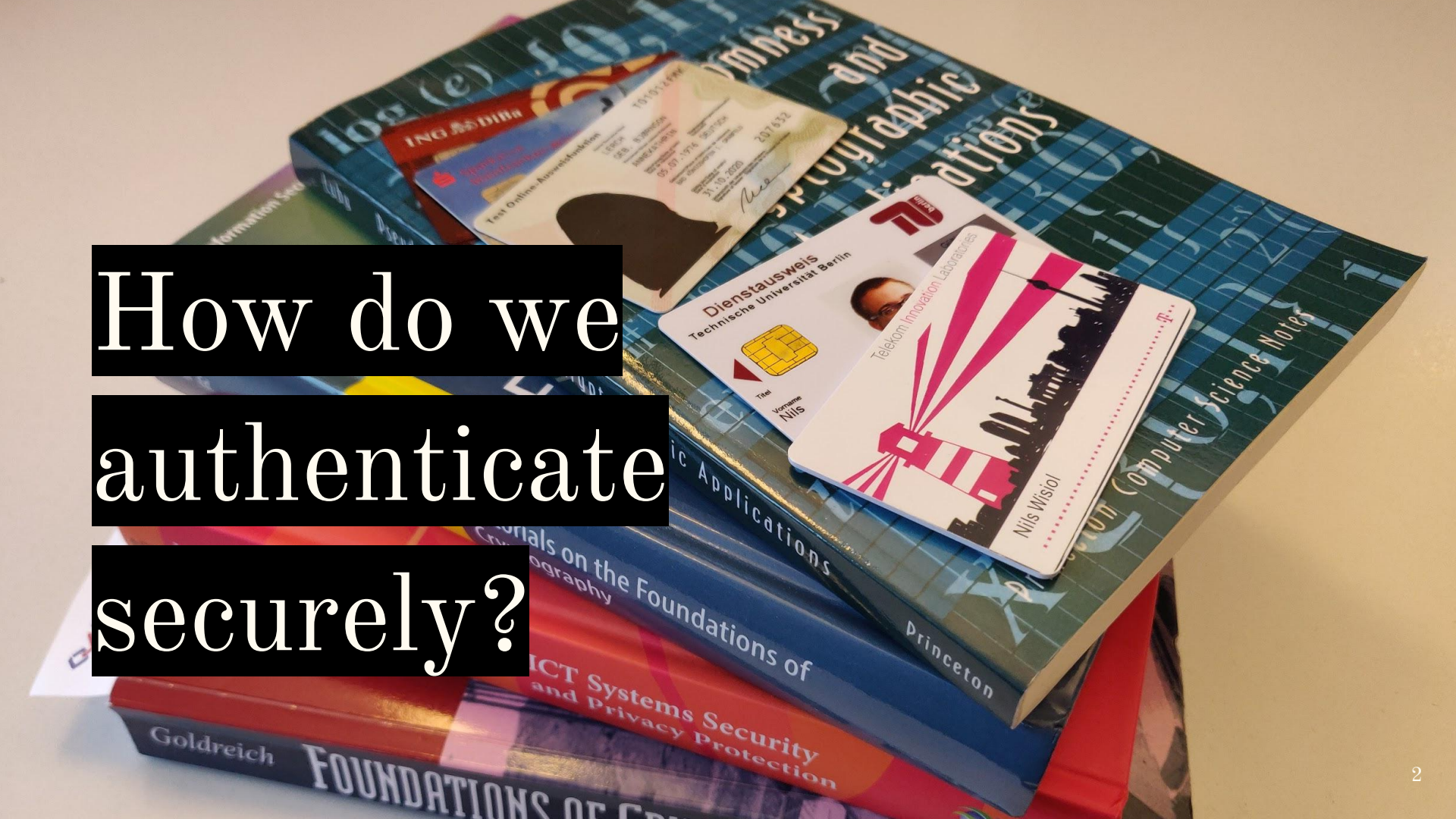
Towards Secure Strong PUFs

Nils Wisiol · 31st Crypto Day · {Freie, Technische} Universität Berlin · nils.wisiol@fu-berlin.de · 17th October 2019

How do we authenticate securely?



A Basic Way

Oh, hey, who are you?

I am card #1337

The MAC Way

secret

What's the answer for *nonce*?

The answer is $f(secret, nonce)$

The Public Key Way

public key

What's the answer for *nonce*?

The answer is $f(secret, nonce)$

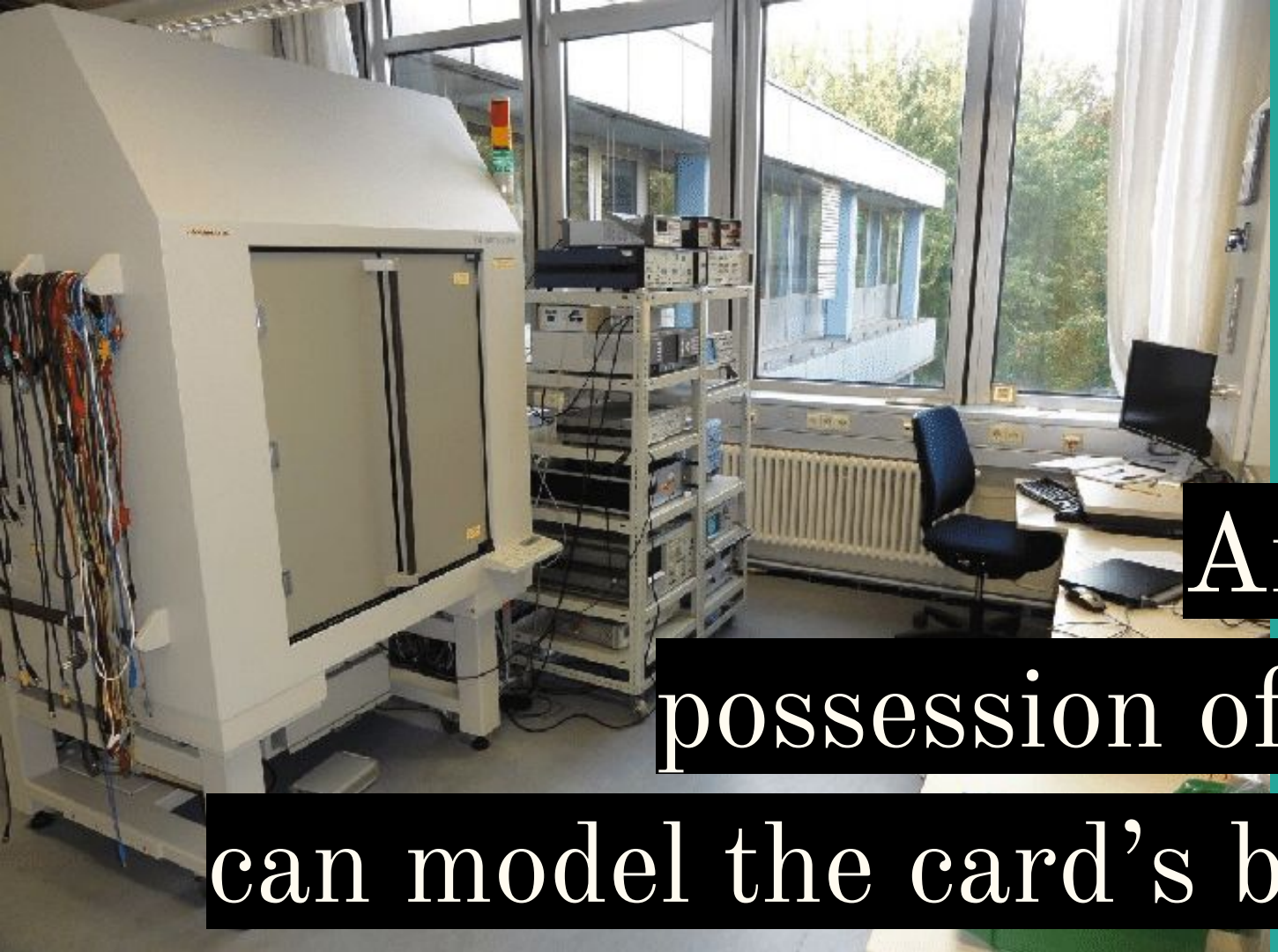
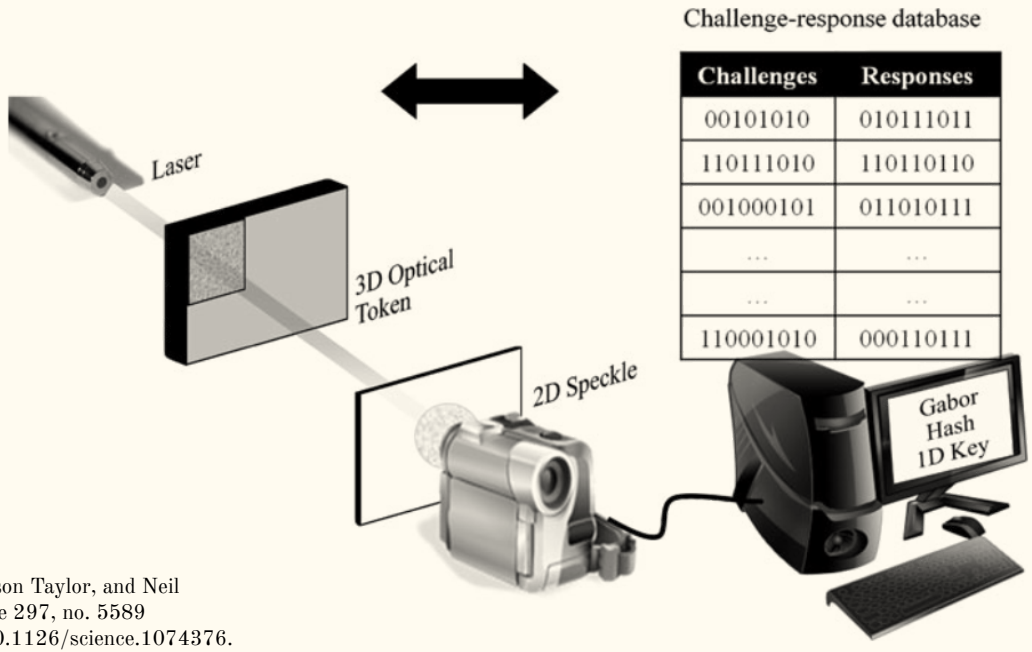


Image source: Scholz, Philipp. “Focused Ion Beam Created Refractive and Diffractive Lens Techniques for the Improvement of Optical Imaging through Silicon,” 2012. https://doi.org/10.14279/depositonce-3270.

Anyone in possession of the key can model the card’s behavior!

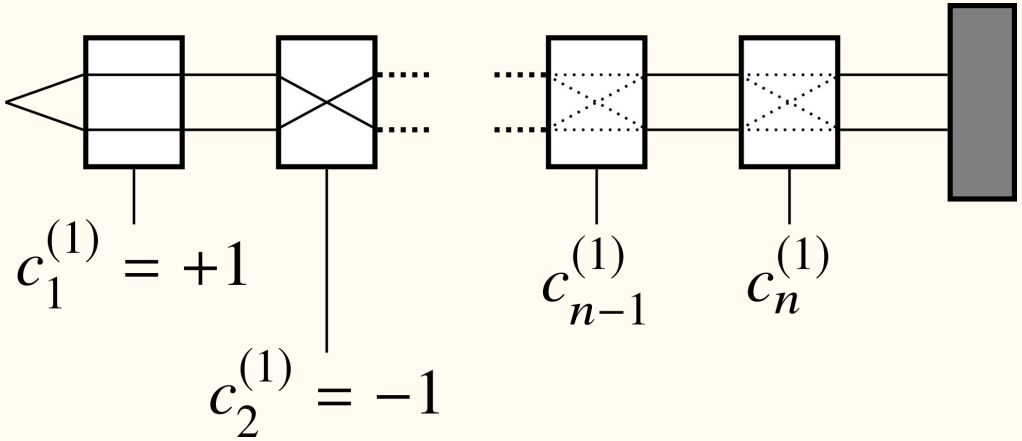
Optical Physically Unclonable Functions



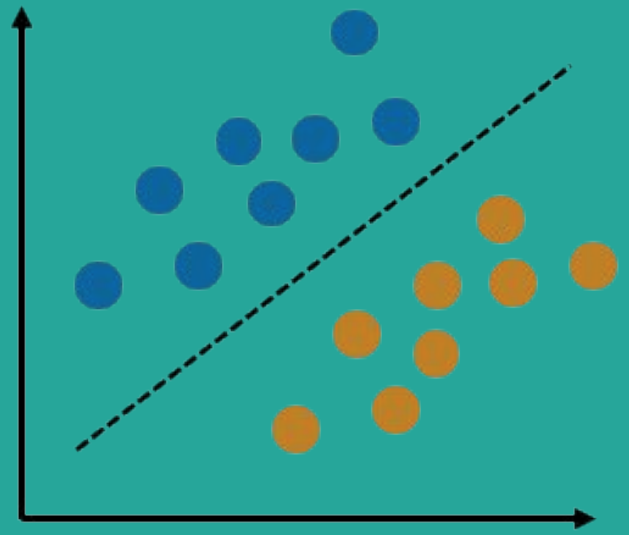
Original research: Pappu, Ravikanth, Ben Recht, Jason Taylor, and Neil Gershenfeld. “Physical One-Way Functions.” Science 297, no. 5589 (September 20, 2002): 2026–30. https://doi.org/10.1126/science.1074376.

Image source: Rührmair, Ulrich, Srinivas Devadas, and Farinaz Koushanfar. “Security Based on Physical Unclonability and Disorder.” In Introduction to Hardware Security and Trust, edited by Mohammad Tehranipoor and Cliff Wang, 65–102. New York, NY: Springer New York, 2012. https://doi.org/10.1007/978-1-4419-8080-9_4.

Arbiter Physical Unclonable Functions (Electric)

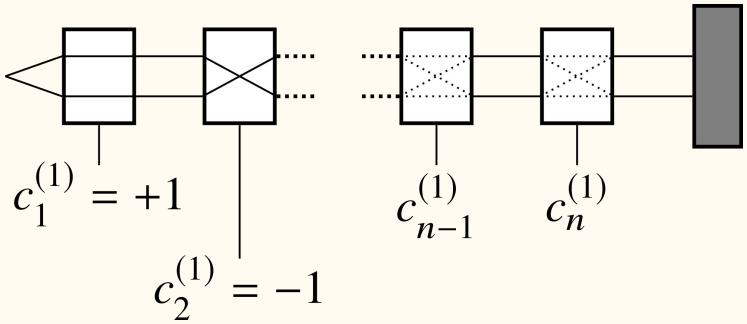


Gassend, Blaise, Dwaine Clarke, Marten van Dijk, and Srinivas Devadas. “Delay-Based Circuit Authentication and Applications.” In Proceedings of the 2003 ACM Symposium on Applied Computing, 294–301. SAC ’03. New York, NY, USA: ACM, 2003. https://doi.org/10.1145/952532.952593.



Can the behavior be modeled?

Arbiter Physical Unclonable Functions (Electric)



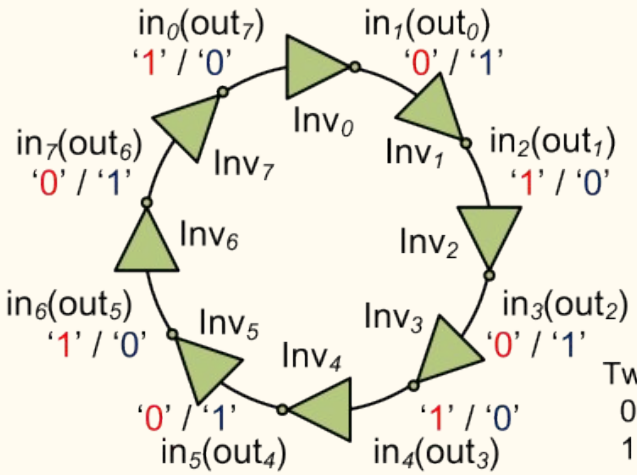
Challenge – attacker known

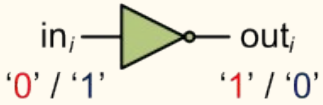
$$\mathrm{sgn}\,\langle w, x \rangle$$

Physical parameters – attacker unknown

Gassend, Blaise, Dwaine Clarke, Marten van Dijk, and Srinivas Devadas. “Delay-Based Circuit Authentication and Applications.” In Proceedings of the 2003 ACM Symposium on Applied Computing, 294–301. SAC ’03. New York, NY, USA: ACM, 2003. https://doi.org/10.1145/952532.952593.

Bistable Ring PUF





Two possible final stable states ($out_0 \ldots out_7$):

$01010101_{BIN} = 55_{HEX}$ ("5"-state)

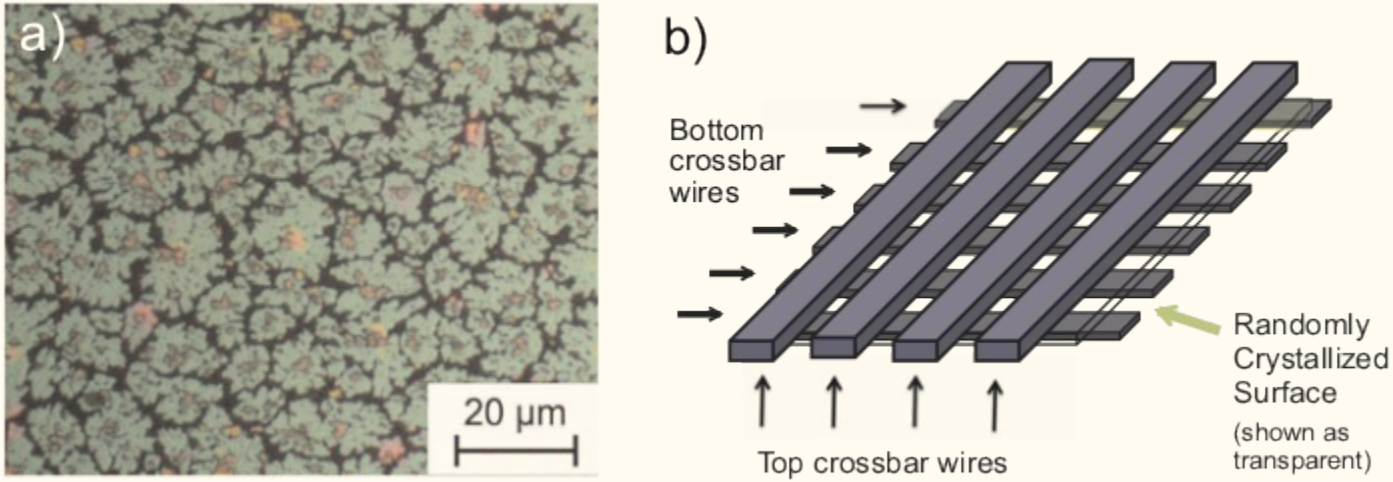
$10101010_{BIN} = AA_{HEX}$ ("A"-state)

Chen, Qingqing, Gyorgy Csaba, Paolo Lugli, Ulf Schlichtmann, and Ulrich Ruhrmair. "The Bistable Ring PUF: A New Architecture for Strong Physical Unclonable Functions." In 2011 IEEE International Symposium on Hardware-Oriented Security and Trust, 134–41. San Diego, CA, USA: IEEE, 2011. https://doi.org/10.1109/HST.2011.5955011.

Schuster, Dieter, and Robert Hesselbarth. "Evaluation of Bistable Ring PUFs Using Single Layer Neural Networks." In Trust and Trustworthy Computing, edited by Thorsten Holz and Sotiris Ioannidis, 101–9. Lecture Notes in Computer Science. Springer International Publishing, 2014.

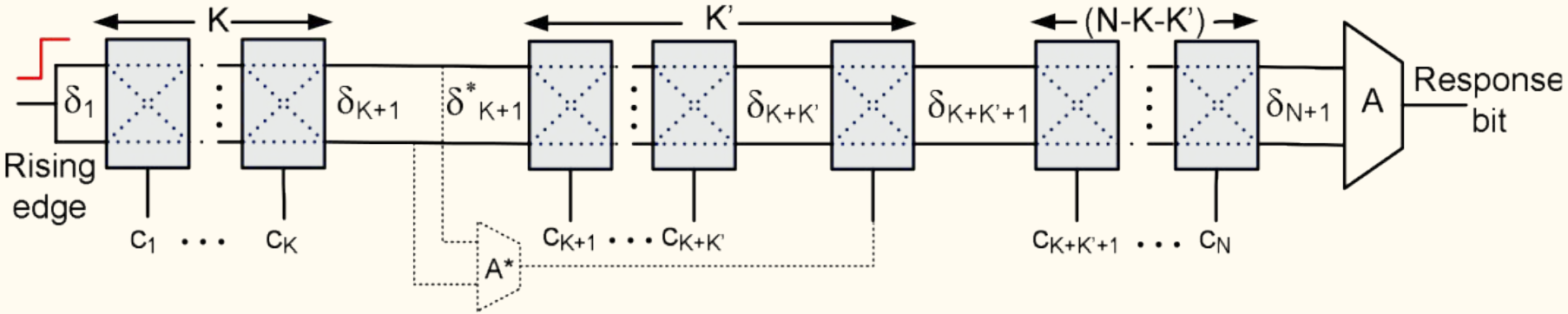
Ganji, Fatemeh, Shahin Tajik, Fabian Fäßler, and Jean-Pierre Seifert. "Strong Machine Learning Attack Against PUFs with No Mathematical Model." In Cryptographic Hardware and Embedded Systems – CHES 2016, edited by Benedikt Gierlichs and Axel Y. Poschmann, 391–411. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2016.

SHIC PUFs



Rührmair, Ulrich. "Oblivious Transfer Based on Physical Unclonable Functions." In Trust and Trustworthy Computing, edited by Alessandro Acquisti, Sean W. Smith, and Ahmad-Reza Sadeghi, 430–40. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2010.

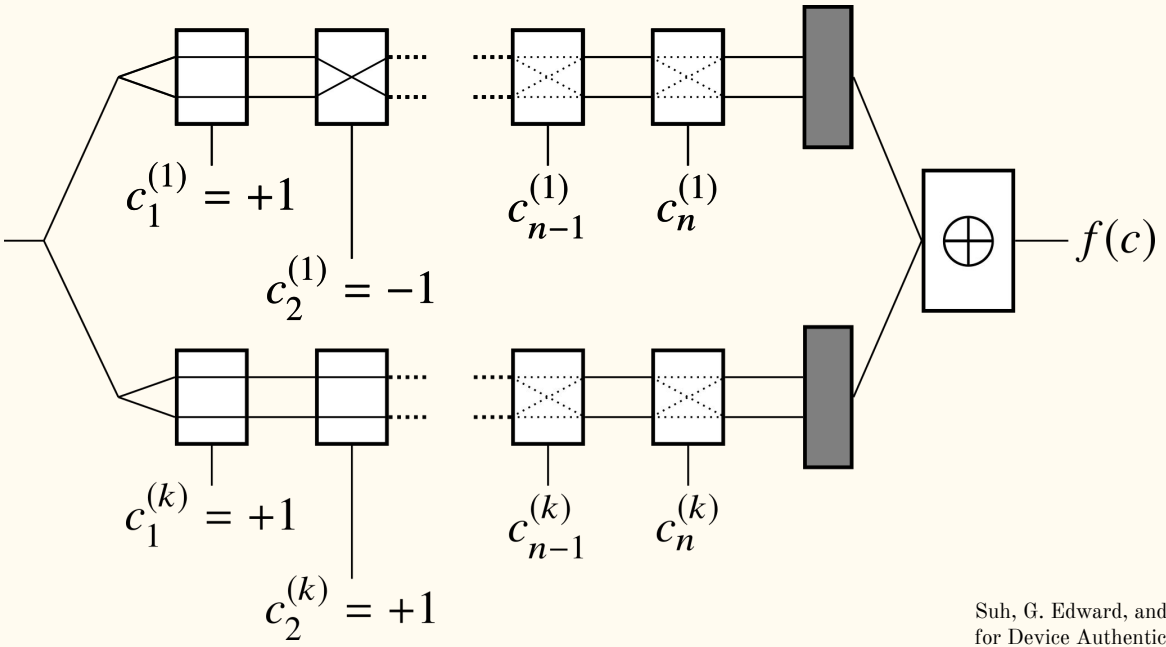
Arbiter PUF Variants: Feed Forward Arbiter PUF



Gassend, Blaise, Daihyun Lim, Dwaine Clarke, Marten van Dijk, and Srinivas Devadas. "Identification and Authentication of Integrated Circuits." Concurrency and Computation: Practice and Experience 16, no. 11 (September 1, 2004): 1077–98. https://doi.org/10.1002/cpe.805.

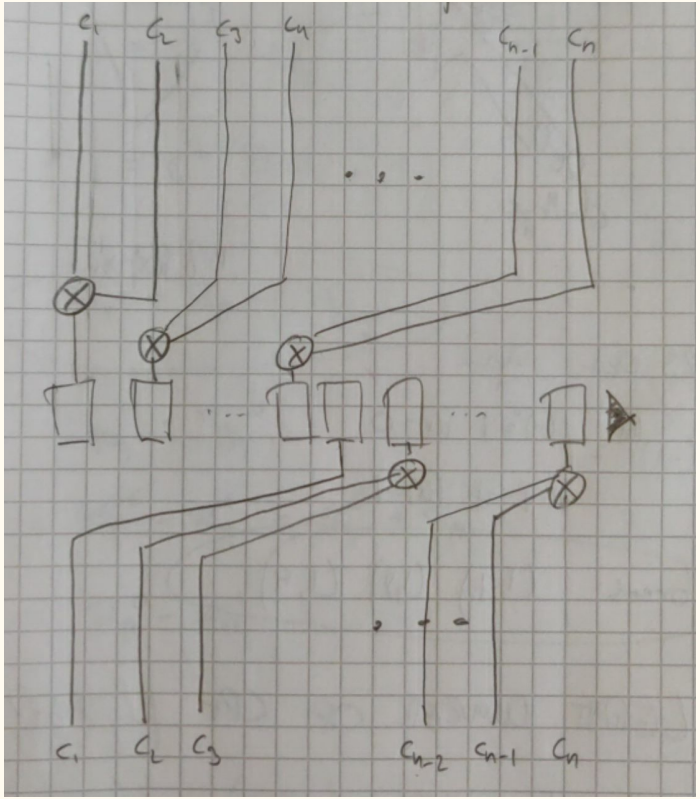
Majzoobi, M., F. Koushanfar, and M. Potkonjak. "Testing Techniques for Hardware Security." In 2008 IEEE International Test Conference, 1–10, 2008. https://doi.org/10.1109/TEST.2008.4700636.

Arbiter PUF Variants: XOR Arbiter PUF



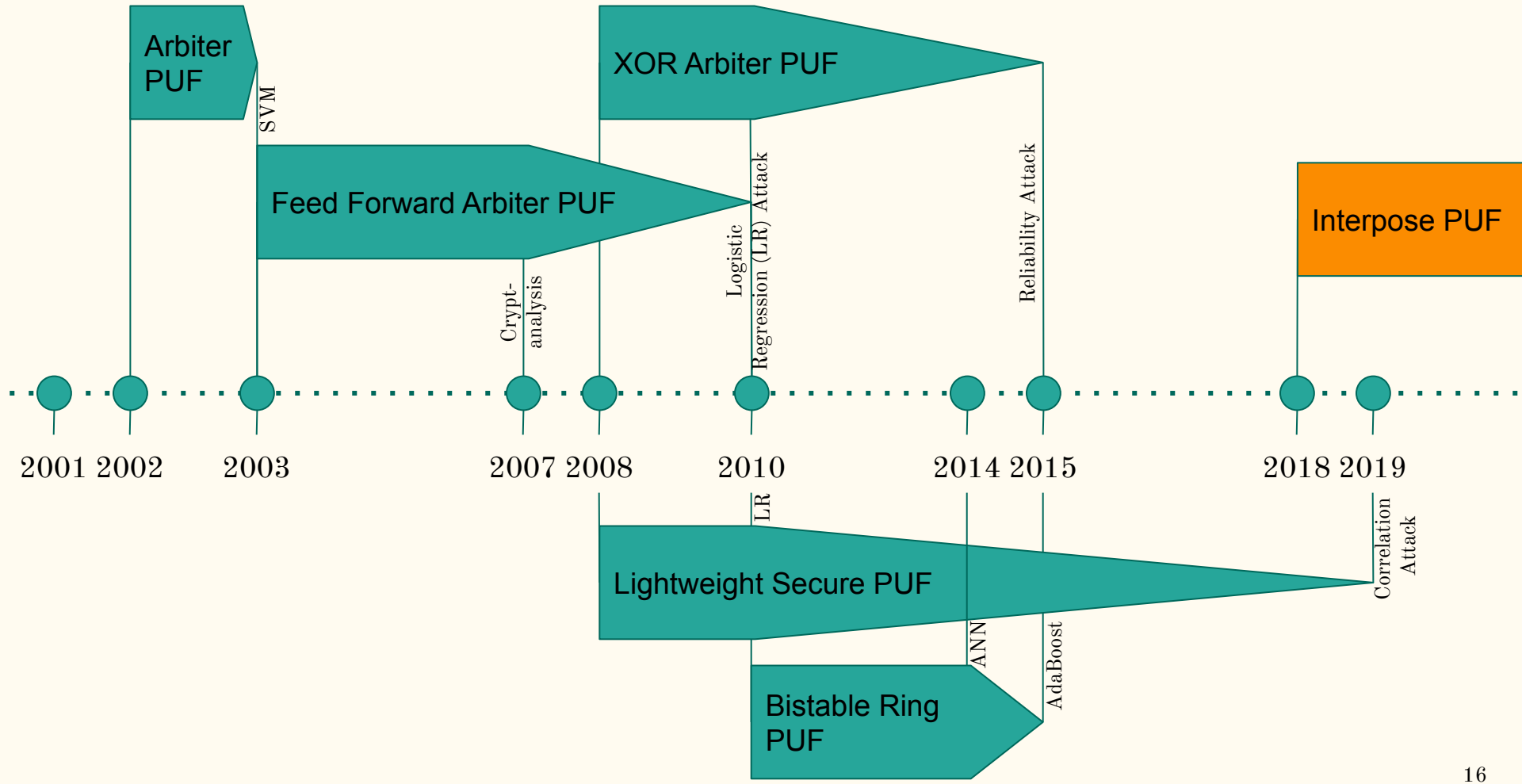
Suh, G. Edward, and Srinivas Devadas. “Physical Unclonable Functions for Device Authentication and Secret Key Generation.” In Proceedings of the 44th Annual Design Automation Conference, 9–14. DAC ’07. New York, NY, USA: ACM, 2007. https://doi.org/10.1145/1278480.1278484.

Lightweight Secure PUF

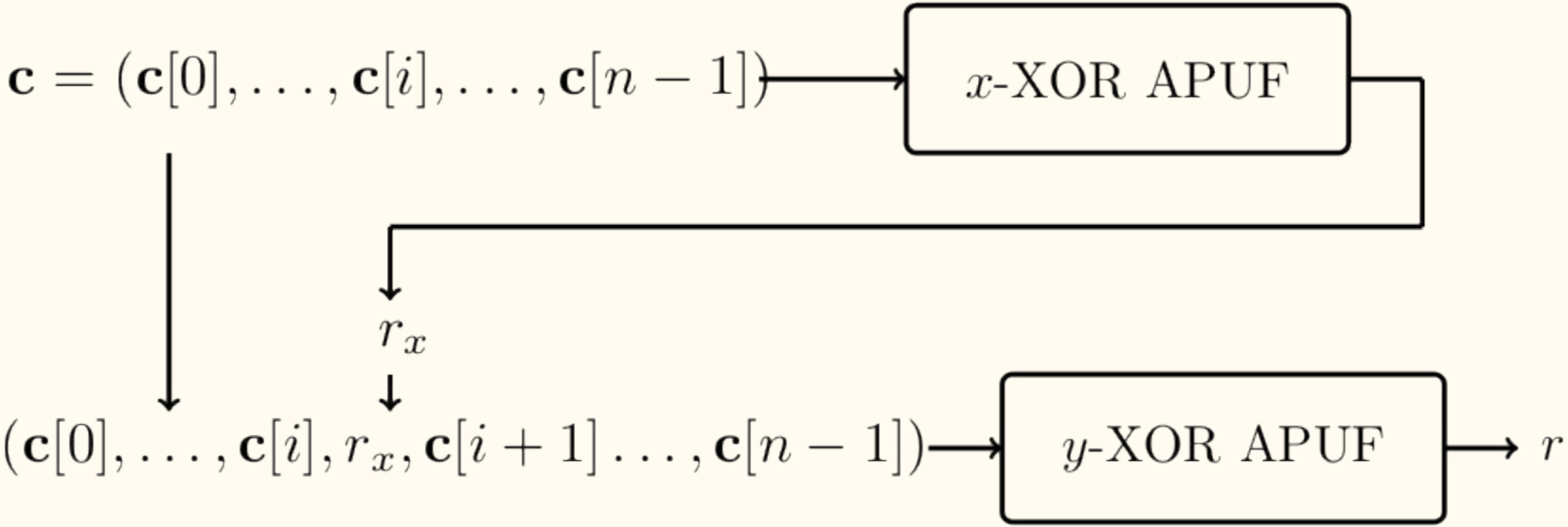


Majzoobi, Mehrdad, Farinaz Koushanfar, and Miodrag Potkonjak. “Lightweight Secure PUFs.” In Proceedings of the 2008 IEEE/ACM International Conference on Computer-Aided Design, 670–673. ICCAD ’08. Piscataway, NJ, USA: IEEE Press, 2008. http://dl.acm.org/citation.cfm?id=1509456.1509603.

Wisiol, Nils, Georg T. Becker, Marian Margraf, Tudor A. A. Soroceanu, Johannes Tobisch, and Benjamin Zengin. “Breaking the Lightweight Secure PUF: Understanding the Relation of Input Transformations and Machine Learning Resistance,” 2019. https://eprint.iacr.org/2019/799.

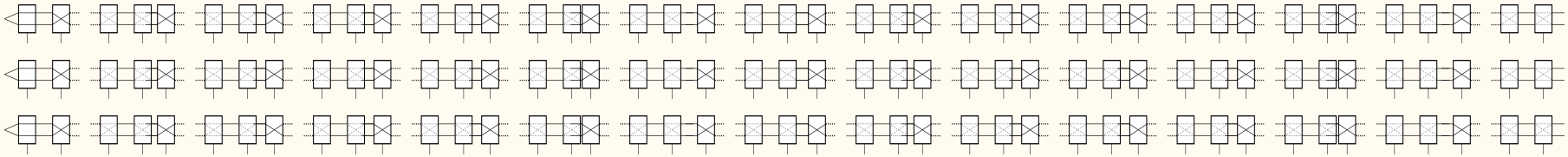

Arbiter PUF
SVM
XOR Arbiter PUF
Feed Forward Arbiter PUF
Crypt-analysis
Logistic Regression (LR) Attack
Reliability Attack
Interpose PUF
2001
2002
2003
2007
2008
2010
2014
2015
2018
2019
LR
Lightweight Secure PUF
Correlation Attack
ANN
AdaBoost
Bistable Ring PUF

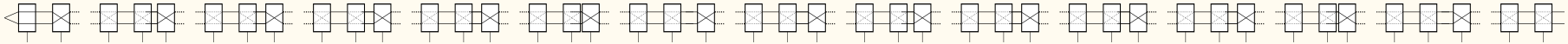
Interpose PUF



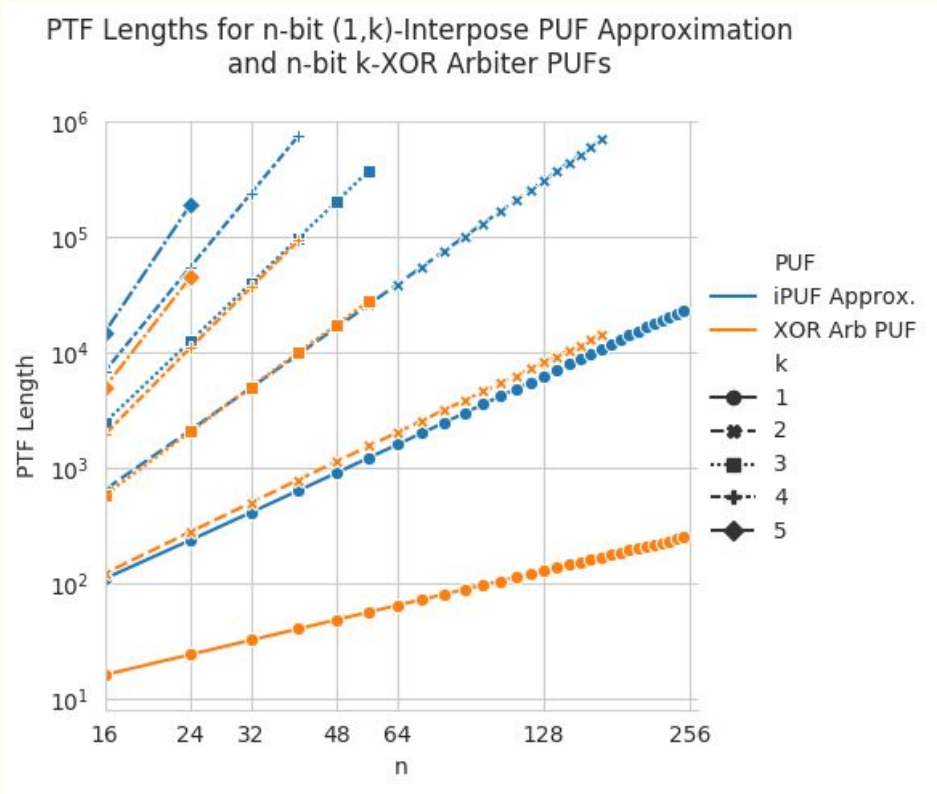
Nguyen, Phuong Ha, Durga Prasad Sahoo, Chenglu Jin, Kaleel Mahmood, Ulrich Rührmair, and Marten van Dijk. "The Interpose PUF: Secure PUF Design against State-of-the-Art Machine Learning Attacks." IACR Transactions on Cryptographic Hardware and Embedded Systems, August 9, 2019, 243–90. https://doi.org/10.13154/tches.v2019.i4.243-290.

Cryptanalysis of the Interpose PUF



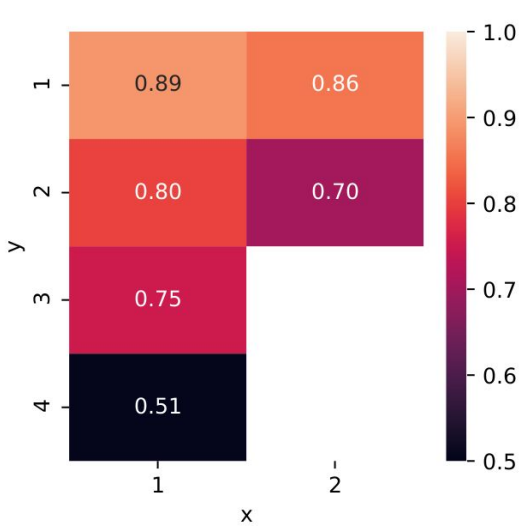


Cryptanalysis of the Interpose PUF

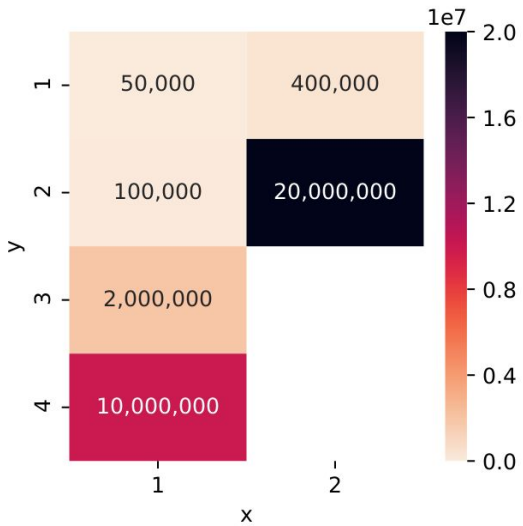


Cryptanalysis of the Interpose PUF (64 bit)

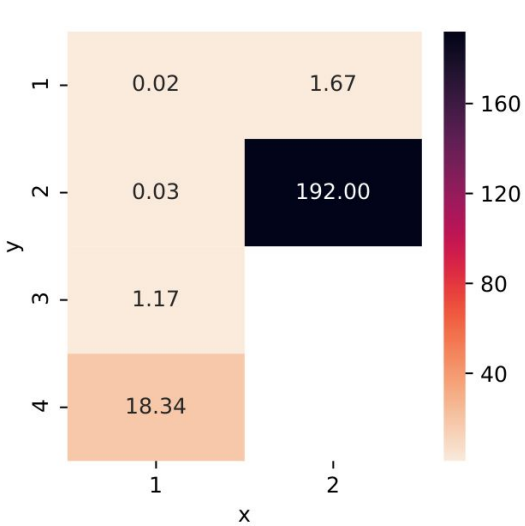
Accuracy



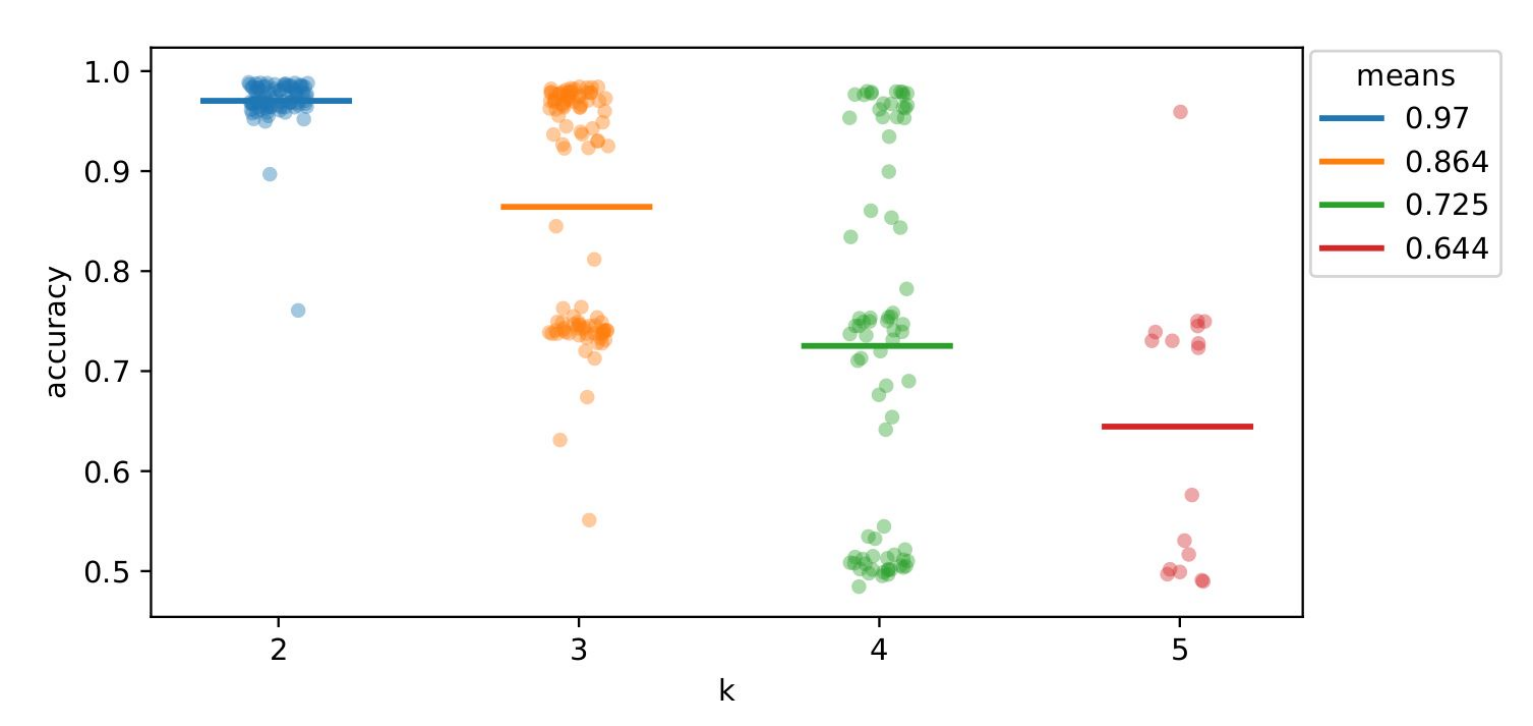
Training Set Size



Run Time (hrs)



Modeling Attack with Deep Learning



Preliminary results; ongoing research with Christopher Mühl

Interpose PUF needs further improvement!

Thanks!

Nils Wisiol · 31st Crypto Day
{Freie, Technische} Universität Berlin
nils.wisiol@fu-berlin.de
17th October 2019
`github.com/nils-wisiol/pypuf`

Discussion

- Multi-bit Outputs?
- Improvement for the Interpose PUF?
- Mitigate Deep Learning Attacks?