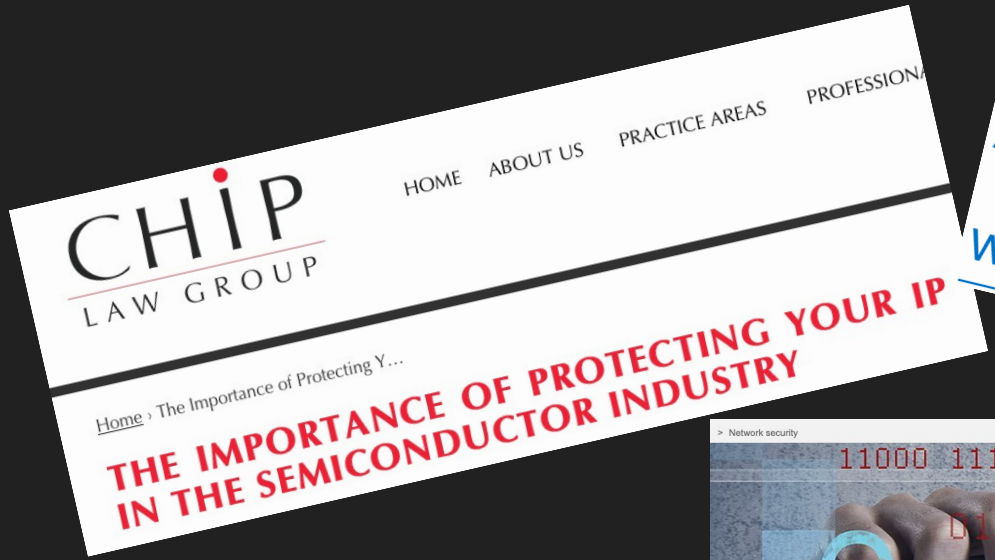
# *FuncTeller*: How Well Does eFPGA Hide Functionality?

Zhaokun Han[1], Mohammed Shayan[2], Aneesh Dixit[1], Mustafa Shihab[2]
Yiorgos Makris[2], and Jeyavijayan (JV) Rajendran[1]

[1] Texas A&M University, [2] The University of Texas at Dallas


# IP Piracy in Hardware Security





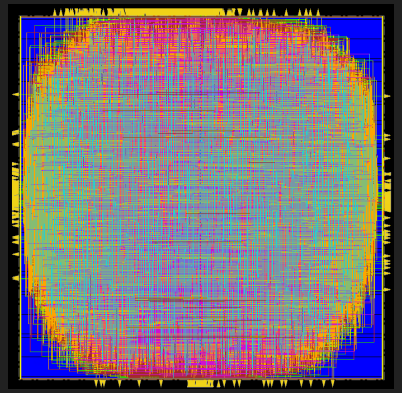

Source: [1]. Chintalapoodi, P. “The Importance of Protecting your IP in the Semiconductor Industry.” Chip Law Group, 2022.
[2]. Areno, M. “Supply Chain Threats Against Integrated Circuits.” Intel Whitepaper, 2020.
[3]. Froehlich, A. “What are the biggest hardware security threats?” TechTarget, 2020.

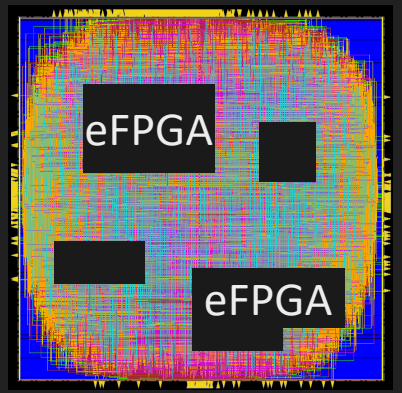
# Hardware Redaction

Original

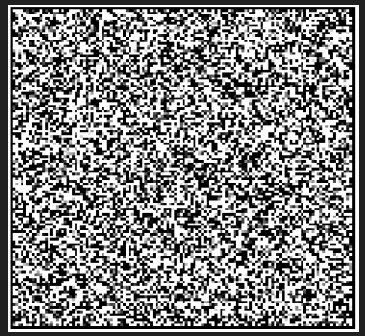
Hardware Redaction

Hardware

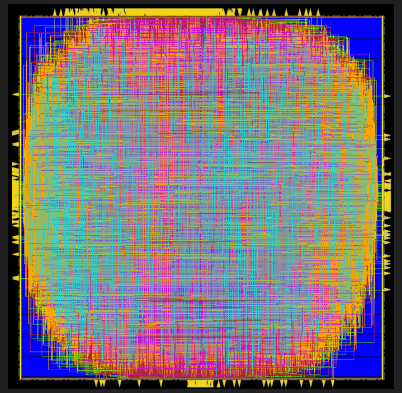
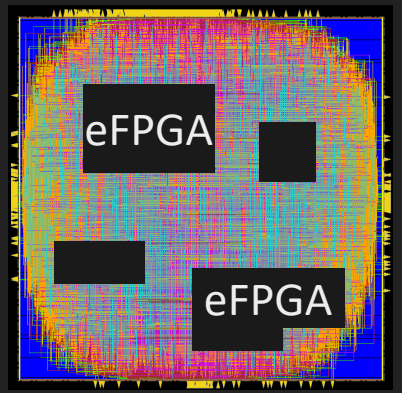
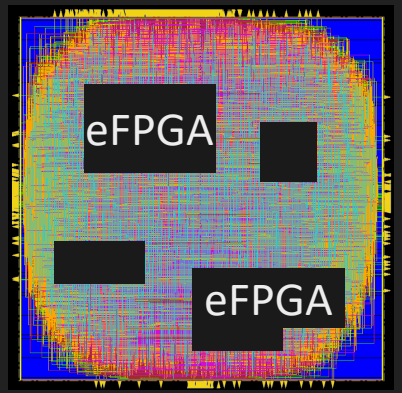
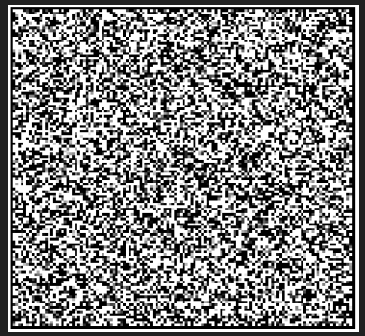




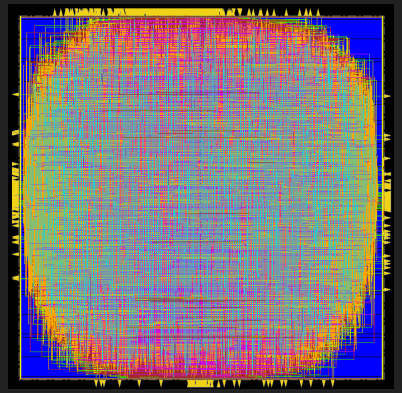
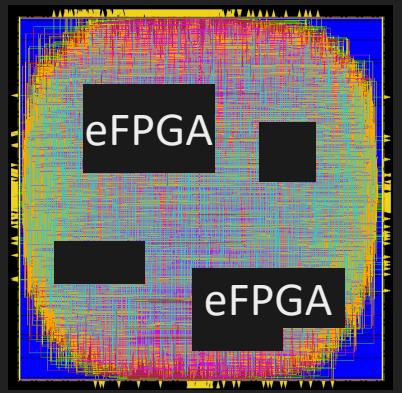
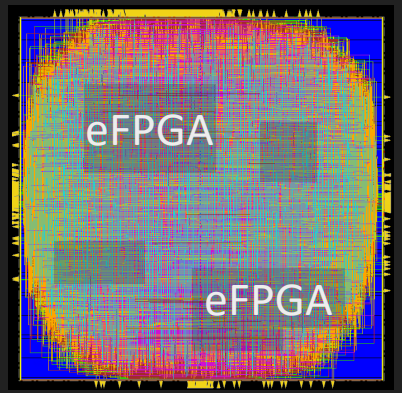
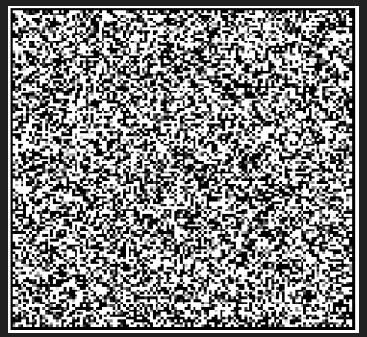

Application behavior



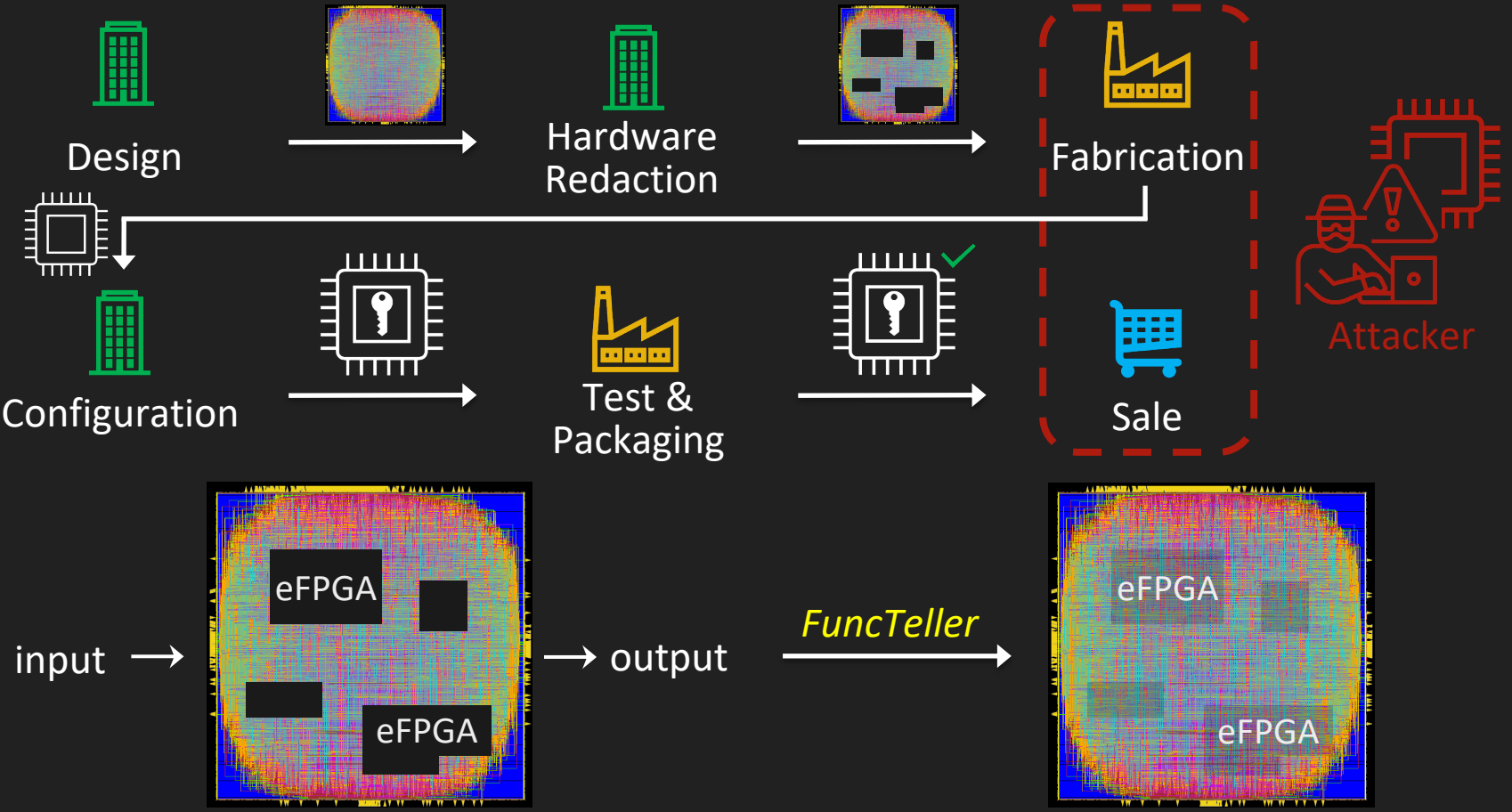
# Hardware Redaction vs. *FuncTeller*

| | Original | Hardware Redaction | *FuncTeller* |
|---|---|---|---|
| Hardware |  |  |  |
| Application behavior |  |  | |

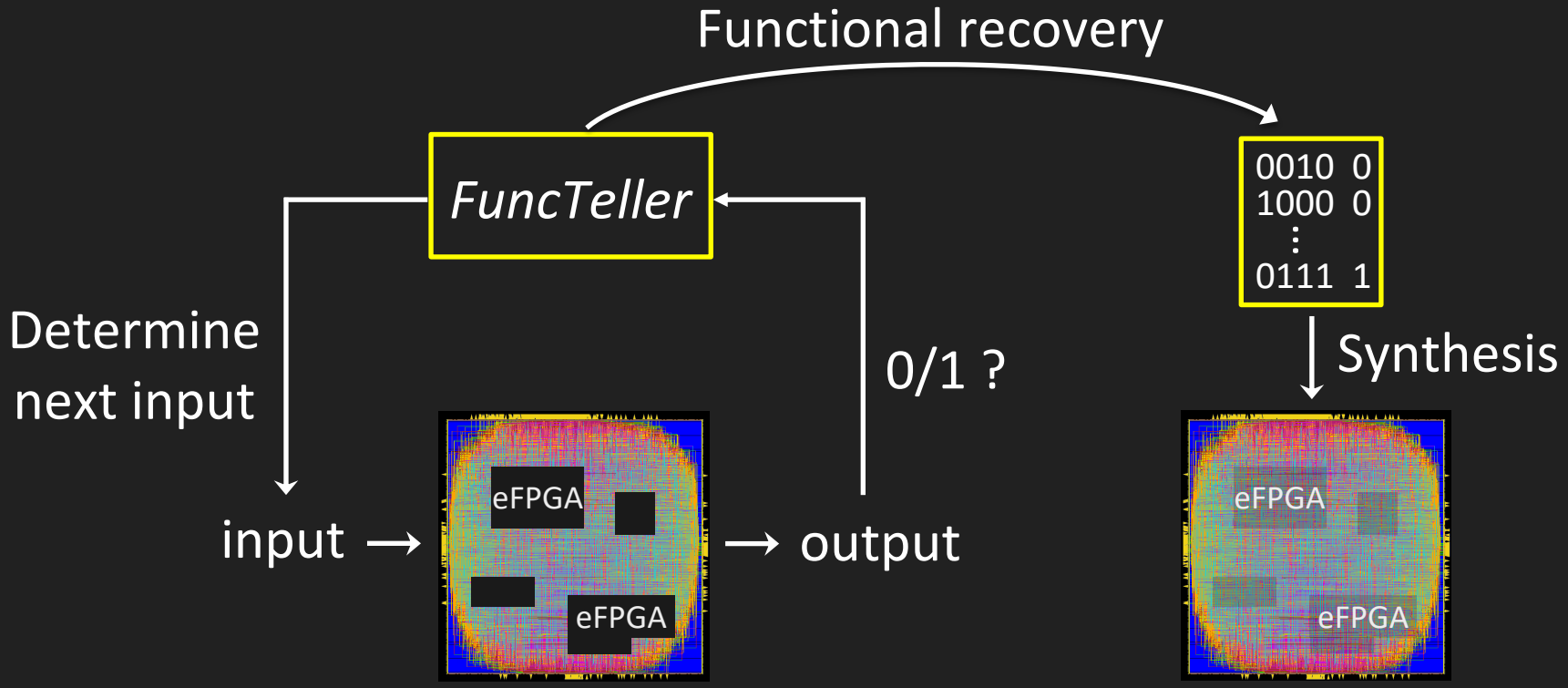
# Hardware Redaction vs. *FuncTeller*

| | Original | Hardware Redaction | *FuncTeller* |
|---|---|---|---|
| Hardware |  |  |  |
| Application behavior |  |  |  |

# Redaction and *FuncTeller* in IC Supply Chain



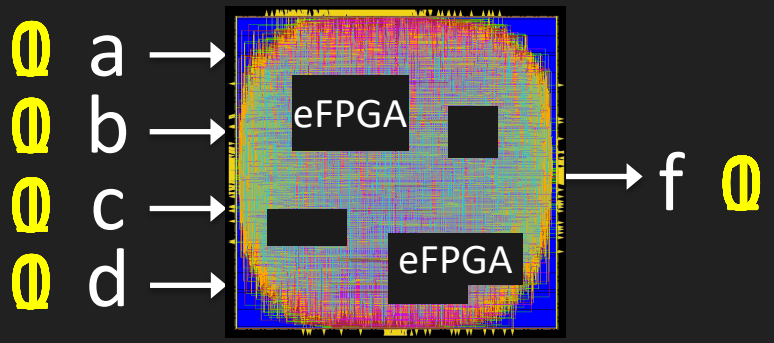
# High-Level Approach




Challenge: exponential query complexity!

# Proposed Attack: *FuncTeller*

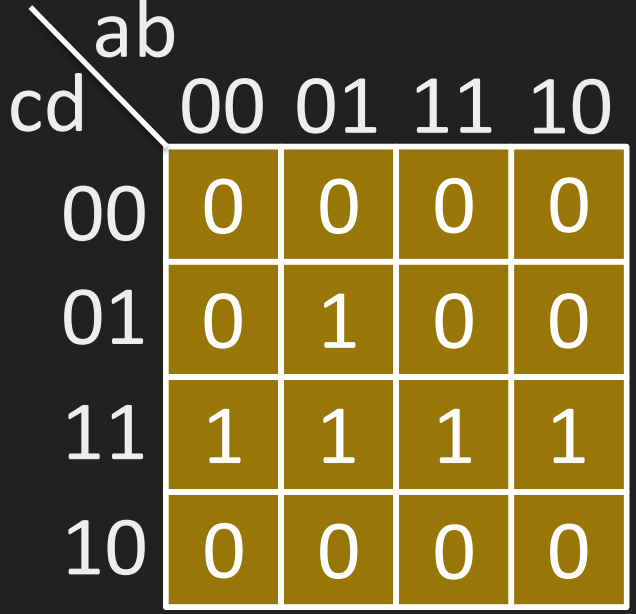
| cd \ ab | 00 | 01 | 11 | 10 |
|---|---|---|---|---|
| 00 | 0 | 0 | 0 | 0 |
| 01 | 0 | 1 | 0 | 0 |
| 11 | 1 | 1 | 1 | 1 |
| 10 | 0 | 0 | 0 | 0 |




Observation: 1s are clustered, and clusters distribute closely!

# Proposed Attack: *FuncTeller*

Random query

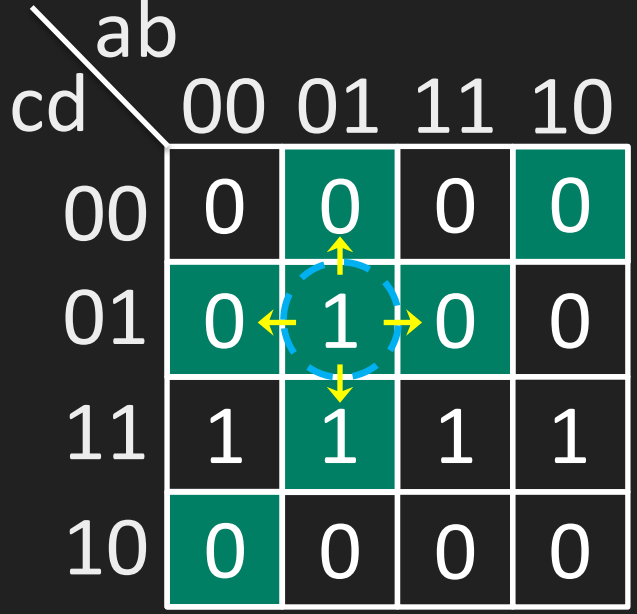


# Proposed Attack: *FuncTeller*

Random query

| cd \ ab | 00 | 01 | 11 | 10 |
|---|---|---|---|---|
| 00 | 0 | 0 | 0 | 0 |
| 01 | 0 | 1 | 0 | 0 |
| 11 | 1 | 1 | 1 | 1 |
| 10 | 0 | 0 | 0 | 0 |

*FuncTeller*

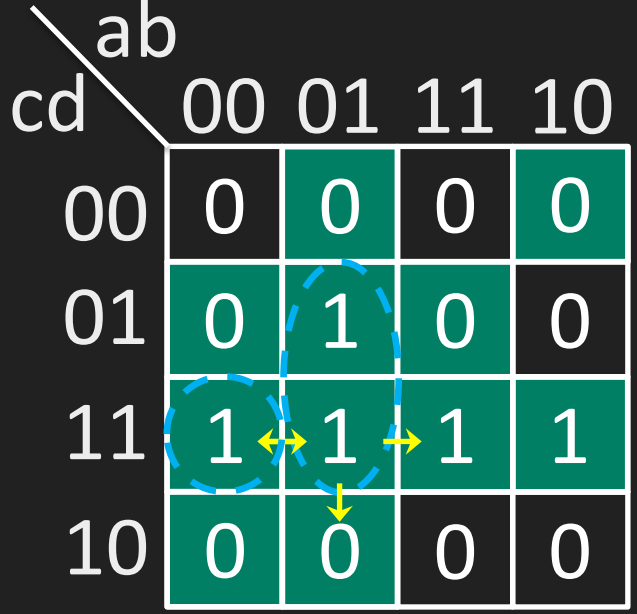


# Proposed Attack: *FuncTeller*

Random query

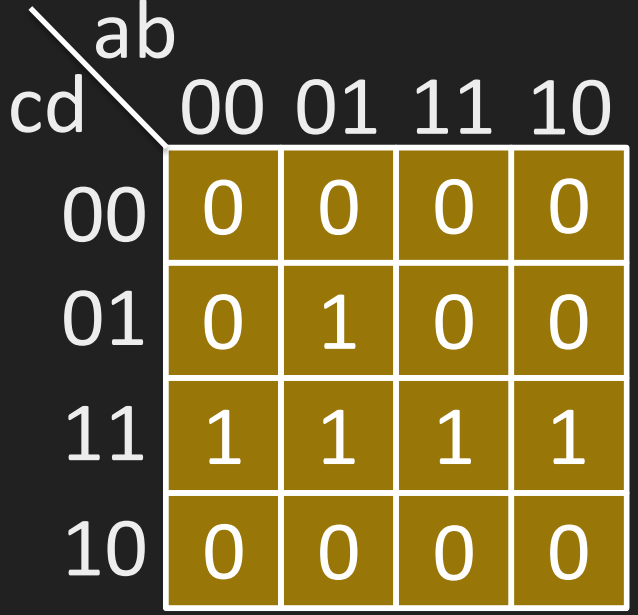
| cd \ ab | 00 | 01 | 11 | 10 |
|---|---|---|---|---|
| 00 | 0 | 0 | 0 | 0 |
| 01 | 0 | 1 | 0 | 0 |
| 11 | 1 | 1 | 1 | 1 |
| 10 | 0 | 0 | 0 | 0 |

*FuncTeller*



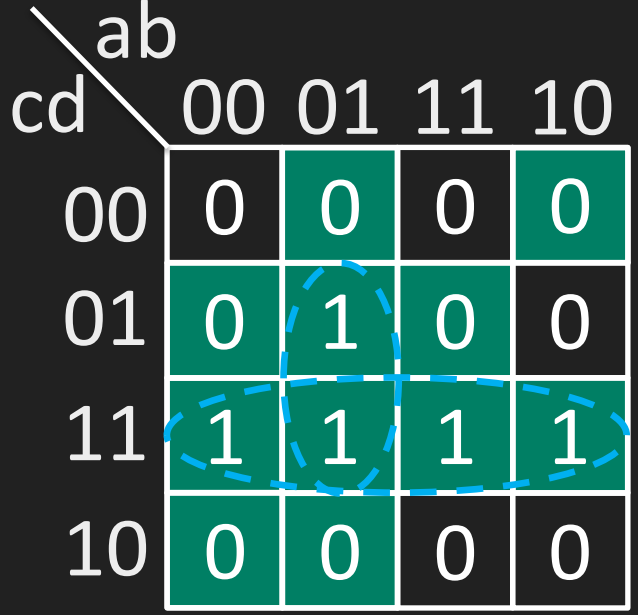
# Proposed Attack: *FuncTeller*

Random query




16 queries

*FuncTeller*




12 queries

# Experimental Results

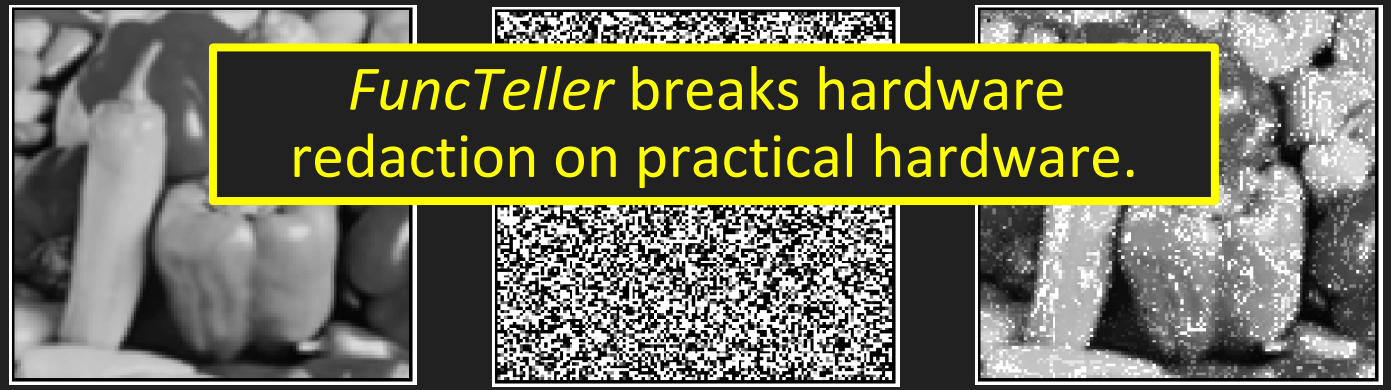
## Performance of *FuncTeller*

| | Circuit | # inputs | # outputs | Time (h) | Accuracy (%) |
|---|---|---|---|---|---|
| Academic | c432 | 36 | 7 | 0.09 | 99.86 |
| | c880 | 60 | 26 | 1.06 | 96.12 |
| | c1355 | 41 | 32 | 1.01 | 50.77 |
| | c1908 | 33 | 25 | 1.00 | 81.82 |
| | c7552 | 207 | 107 | 1.25 | 86.66 |
| | b14 | 277 | 299 | 1.39 | 92.46 |
| | b20 | 522 | 512 | 9.92 | 84.10 |
| Industrial | MIPS | 430 | 407 | 1.84 | 95.49 |
| | IBEX | 1,386 | 1,385 | 72.85 | 90.96 |
| | GPS | 9,707 | 9,731 | 44.44 | 68.89 |

Accuracy **> 90%** on the IBEX processor

# Real-World Application

Gaussian blur on the image with image processing circuit



*FuncTeller* breaks hardware redaction on practical hardware.

Golden | Redacted | *FuncTeller*



# *Thank you!!*

SCAN ME

Zhaokun Han

hzhk0618@tamu.edu

https://linkedin.com/in/zhaokun-han

TAMU SETH Lab

https://seth.engr.tamu.edu