DESIGN AUTOMATION CONFERENCE

58

FROM CHIPS TO SYSTEMS — LEARN TODAY, CREATE TOMORROW

DEC 5 - 9, 2021 ◆ San Francisco, California

Classifying Computations on Multi-Tenant FPGAs

University of California, San Diego
Mustafa Gobulukoglu, Colin Drewes, Ryan Kastner

Georgia Tech Research Institute
Bill Hunter

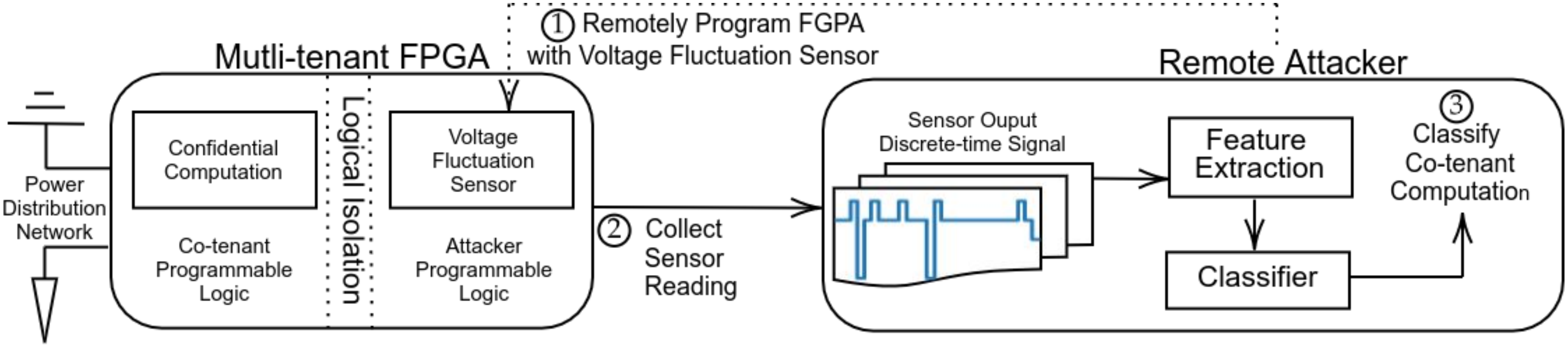
University of Washington
Dustin Richmond

Overview

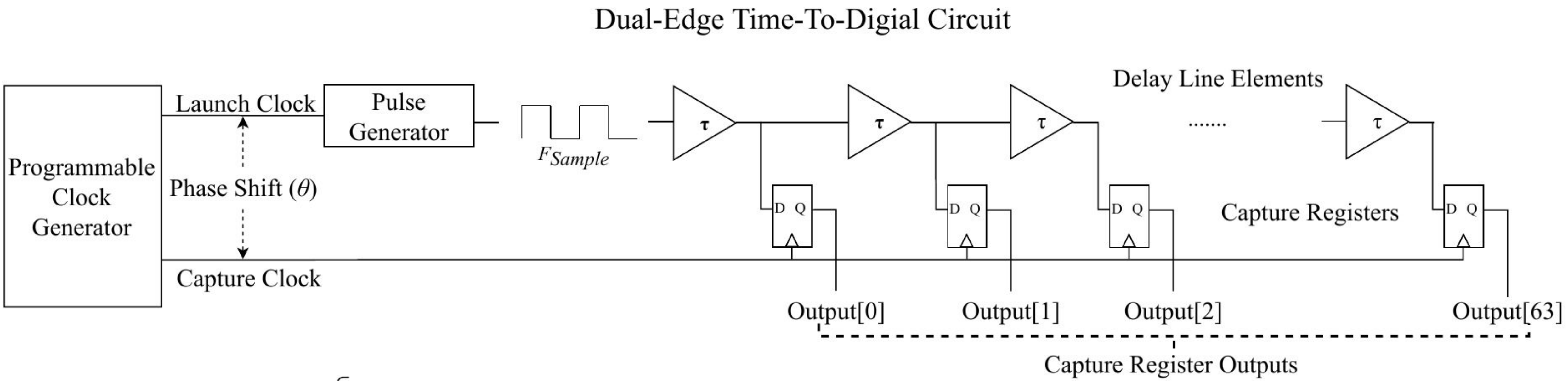
- FPGAs are powerful, but expensive -> virtualization
- Virtualization exposes a side-channel through shared power distribution
- Leverage this to determine aspects of co-located computation

    Type of computation? Implementation?

Proposed Threat-Model



Voltage Fluctuation Sensor



Output Sequence

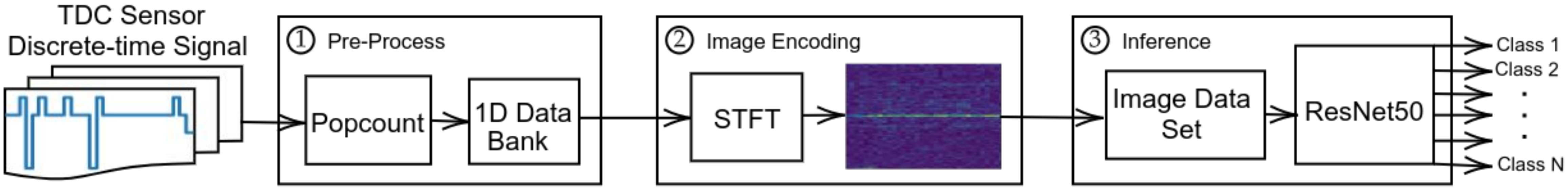
Positive Transition 0: 1111_1111_1111_1111_1111_1111_1111_1111_1111_1100_0000_0000_0000_0000_0000_0000

Negative Transition 0: 0000_0000_0000_0000_0000_1111_1111_1111_1111_1111_1111_1111_1111_1111_1111_1111

Positive Transition 1: 1111_1111_1111_1111_1111_1111_1111_1111_1111_0000_0000_0000_0000_0000_0000_0000

Negative Transition 1: 0000_0000_0000_0000_0000_0011_1111_1111_1111_1111_1111_1111_1111_1111_1111_1111

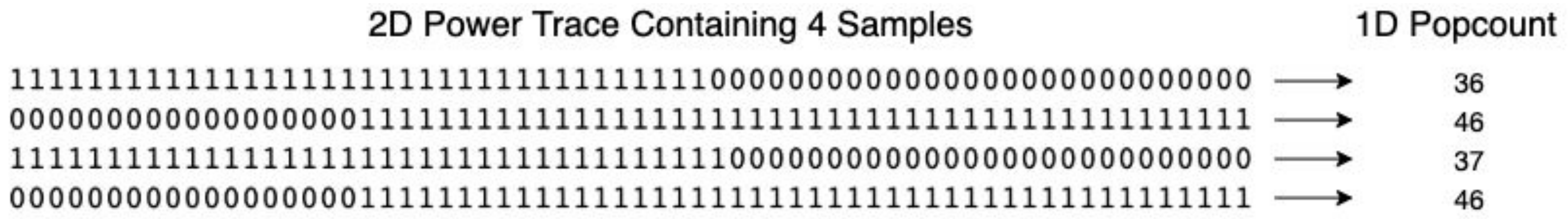
Three-Stage Classification Pipeline



Co-Located Applications

- Baseline
- Power Wasters
- Cryptographic Cores (AES, PRESENT)
  1) Custom IP AES
  2) Orca
  3) PicoRV
  4) Microblaze

① Pre-Process



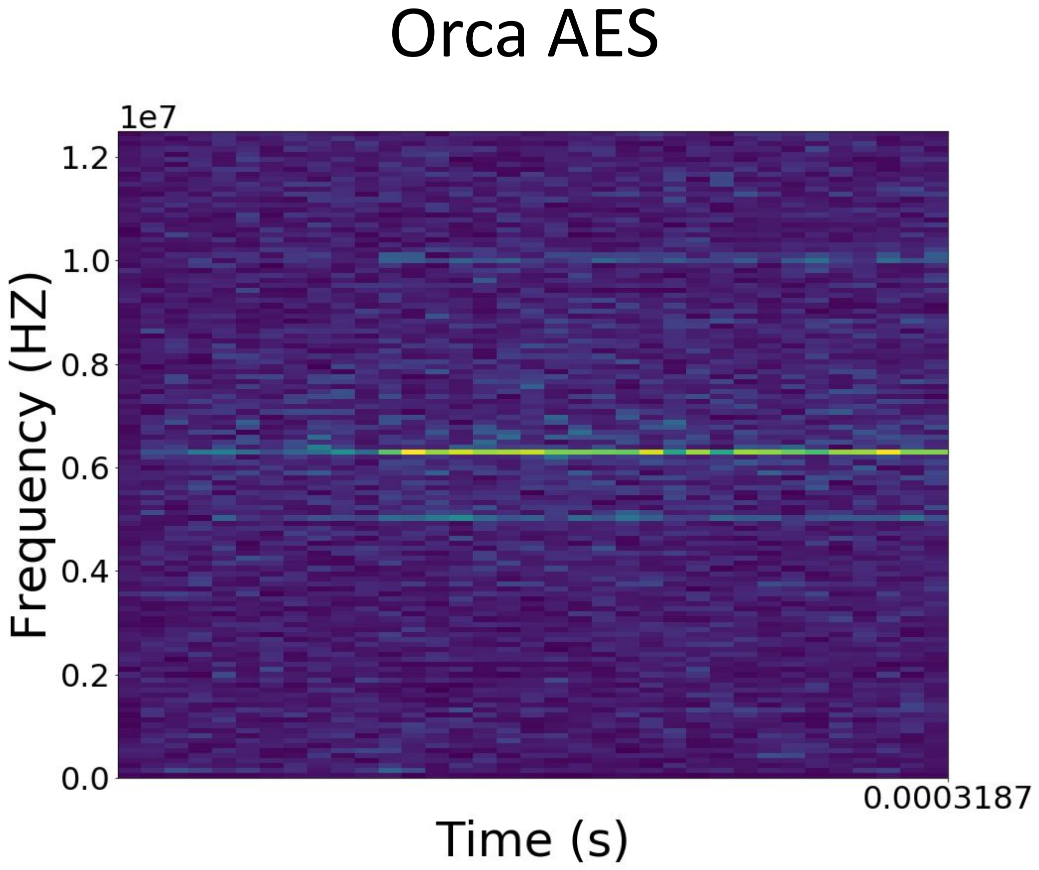
2D Power Trace Containing 4 Samples

1D Popcount

```
1111111111111111111111111111111111110000000000000000000000000000  ⟶  36
0000000000000000001111111111111111111111111111111111111111111111  ⟶  46
1111111111111111111111111111111111111000000000000000000000000000  ⟶  37
0000000000000000001111111111111111111111111111111111111111111111  ⟶  46
```

② Image Encoding: STFT

- Fourier transforms over windows of signal
- Produce an image that encodes the frequency domain of the signal at a given time
- Wish to encode aspects of co-tenant’s computations

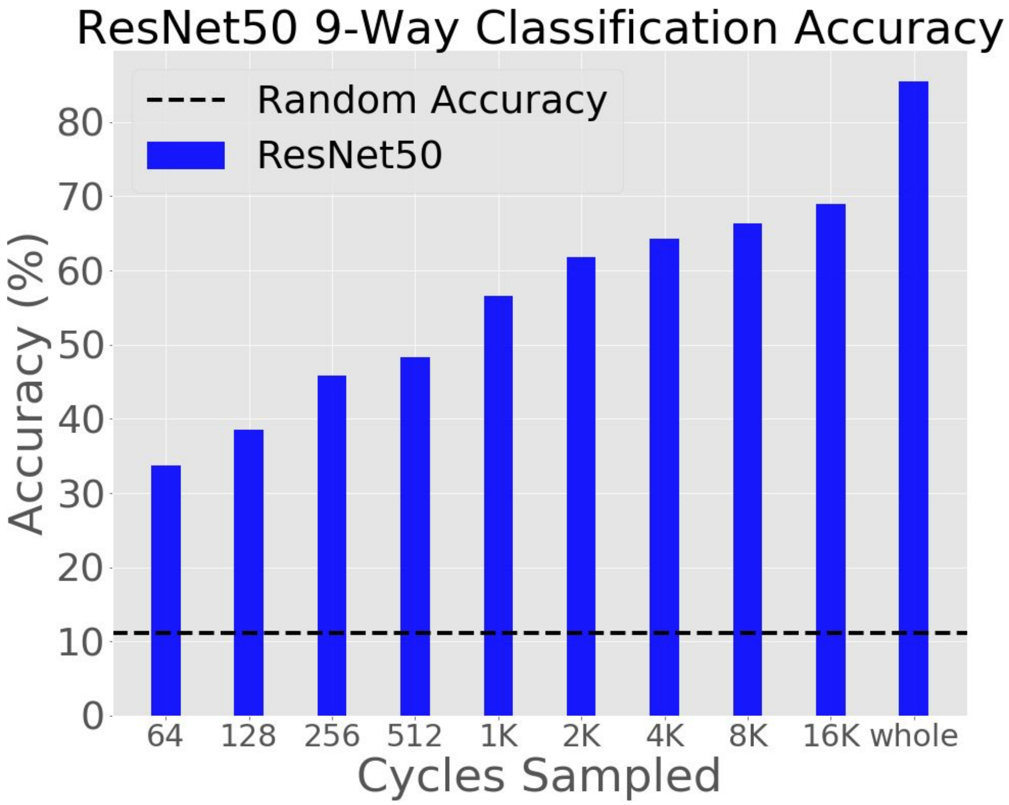


③ Classification: ResNet50

- Convolutional Neural Network
- Images ⟶ Labels (baseline, power wasters, AES, PRESENT, Orca,...)
- Trained on labeled STFT images from the 9 classes
- Tested on reserved set of STFTs from the 9 classes

Classification Accuracy

- 9-way classification accuracy
- Duration of sampling matters
- Longer segments → Better Accuracy



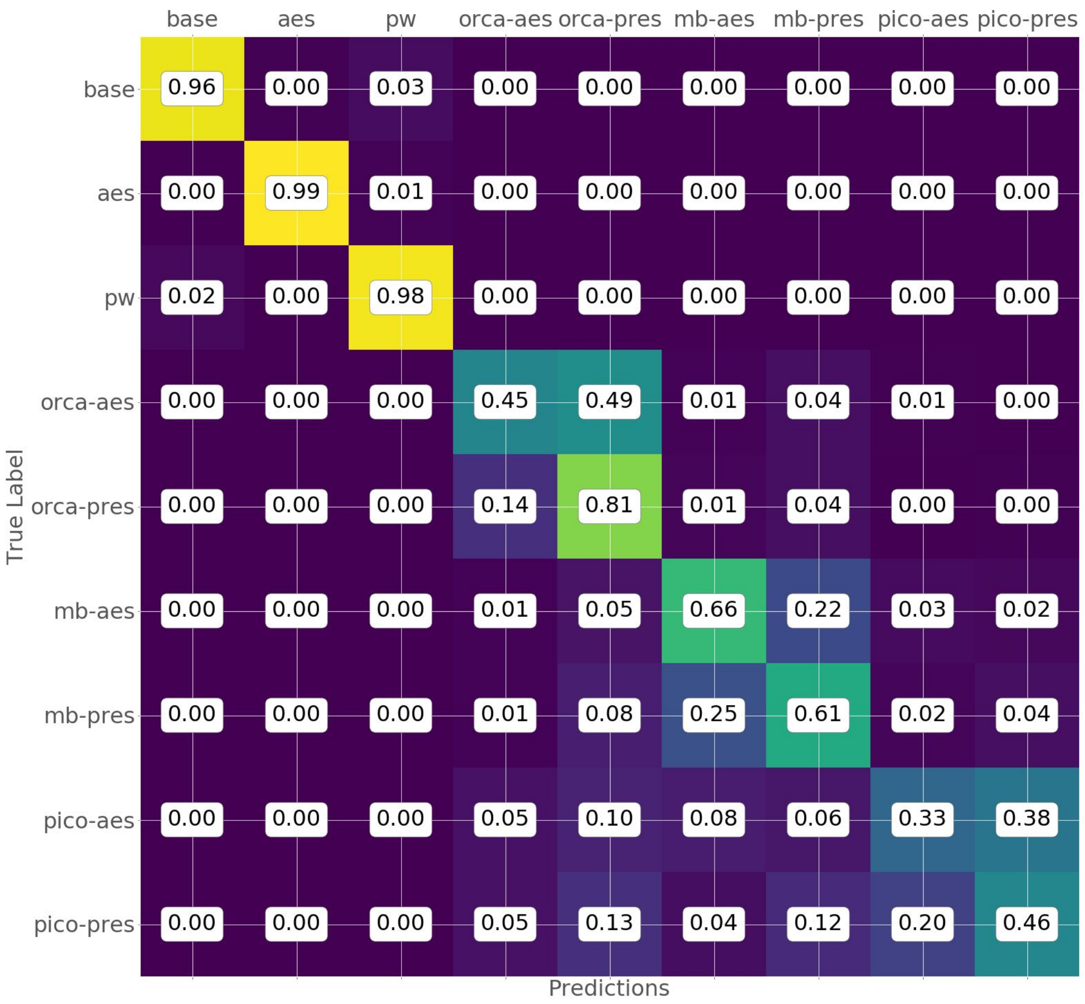
Confusion

- Strong classification between

  base, AES, PW, Orca, PicoRV, MicroBlaze

- Misclassification between applications on

  single soft-processors



	base	aes	pw	orca-aes	orca-pres	mb-aes	mb-pres	pico-aes	pico-pres
base	0.96	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.00
aes	0.00	0.99	0.01	0.00	0.00	0.00	0.00	0.00	0.00
pw	0.02	0.00	0.98	0.00	0.00	0.00	0.00	0.00	0.00
orca-aes	0.00	0.00	0.00	0.45	0.49	0.01	0.04	0.01	0.00
orca-pres	0.00	0.00	0.00	0.14	0.81	0.01	0.04	0.00	0.00
mb-aes	0.00	0.00	0.00	0.01	0.05	0.66	0.22	0.03	0.02
mb-pres	0.00	0.00	0.00	0.01	0.08	0.25	0.61	0.02	0.04
pico-aes	0.00	0.00	0.00	0.05	0.10	0.08	0.06	0.33	0.38
pico-pres	0.00	0.00	0.00	0.05	0.13	0.04	0.12	0.20	0.46

Conclusions

- Remote attacker can upload TDC and collect sensor readings which reflect other user’s activity in multi-tenant environment

- Proposed three-stage classification for identifying remote computation

- Ability to classify computation is necessary precursor to existing power distribution and side-channel attacks