Turn on, Tune in, Listen up

Maximizing Side-Channel Recovery in Time-to-Digital Converters

Colin Drewes[1], Olivia Weng[1], Keegan Ryan[1], Bill Hunter[2], Christopher McCarty[2], Ryan Kastner[1], and Dustin Richmond[3]

[1]UCSD, [2]GTRI, [3]UCSC

February 13, 2023

FPGAs are powerful...but often prohibitively expensive

FPGAs are powerful...but often prohibitively expensive

This has pushed us towards...

FPGAs are powerful...but often prohibitively expensive

This has pushed us towards...

- Cloud-FPGA leasing schemes (temporal sharing)

FPGAs are powerful...but often prohibitively expensive

This has pushed us towards...

- Cloud-FPGA leasing schemes (temporal sharing)
- Integration of proprietary IP

FPGAs are powerful...but often prohibitively expensive

This has pushed us towards...

- Cloud-FPGA leasing schemes (temporal sharing)
- Integration of proprietary IP
- Full FPGA virtualization (temporospatial sharing)

FPGAs are powerful...but often prohibitively expensive

This has pushed us towards...

- Cloud-FPGA leasing schemes (temporal sharing)
- Integration of proprietary IP
- Full FPGA virtualization (temporospatial sharing)

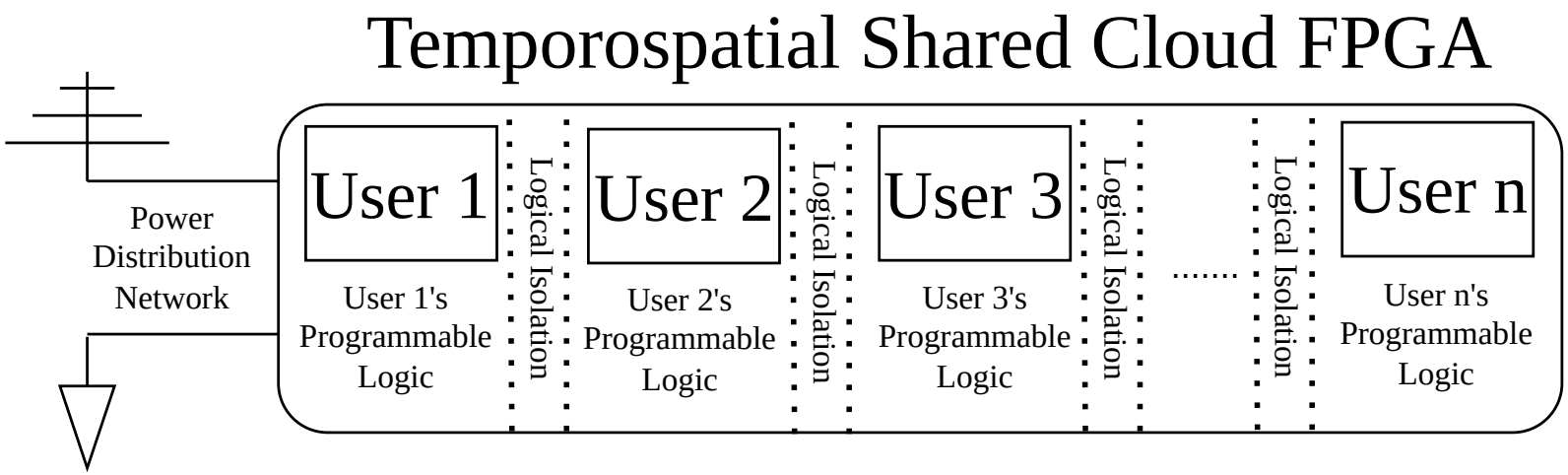
Observation: These are all multi-actor structures—potentially running hidden opaque circuitry.

FPGAs are powerful...but often prohibitively expensive

This has pushed us towards...

- Cloud-FPGA leasing schemes (temporal sharing)
- Integration of proprietary IP
- Full FPGA virtualization (temporospatial sharing)

Observation: These are all multi-actor structures—potentially running hidden opaque circuitry.



FPGAs are powerful...but often prohibitively expensive

This has pushed us towards...

- Cloud-FPGA leasing schemes (temporal sharing)
- Integration of proprietary IP
- Full FPGA virtualization (temporospatial sharing)

Observation: These are all multi-actor structures—potentially running hidden opaque circuitry.

While logical boundaries may be in place, they all share the same power system!

FPGAs are powerful...but often prohibitively expensive

This has pushed us towards...

- Cloud-FPGA leasing schemes (temporal sharing)
- Integration of proprietary IP
- Full FPGA virtualization (temporospatial sharing)

Observation: These are all multi-actor structures—potentially running hidden opaque circuitry.

While logical boundaries may be in place, they all share the same power system!

If a dedicated actor were able to instantiate a voltage fluctuation sensor within their allocated logic they could...

FPGAs are powerful...but often prohibitively expensive

This has pushed us towards...

- Cloud-FPGA leasing schemes (temporal sharing)
- Integration of proprietary IP
- Full FPGA virtualization (temporospatial sharing)

Observation: These are all multi-actor structures—potentially running hidden opaque circuitry.

While logical boundaries may be in place, they all share the same power system!

If a dedicated actor were able to instantiate a voltage fluctuation sensor within their allocated logic they could...

- Determine what core other actors are executing

FPGAs are powerful...but often prohibitively expensive

This has pushed us towards...

- Cloud-FPGA leasing schemes (temporal sharing)
- Integration of proprietary IP
- Full FPGA virtualization (temporospatial sharing)

Observation: These are all multi-actor structures—potentially running hidden opaque circuitry.

While logical boundaries may be in place, they all share the same power system!

If a dedicated actor were able to instantiate a voltage fluctuation sensor within their allocated logic they could...

- Determine what core other actors are executing
- Determine what is running on an actor's soft-processor

FPGAs are powerful...but often prohibitively expensive

This has pushed us towards...

- Cloud-FPGA leasing schemes (temporal sharing)
- Integration of proprietary IP
- Full FPGA virtualization (temporospatial sharing)

Observation: These are all multi-actor structures—potentially running hidden opaque circuitry.

While logical boundaries may be in place, they all share the same power system!

If a dedicated actor were able to instantiate a voltage fluctuation sensor within their allocated logic they could...

- Determine what core other actors are executing
- Determine what is running on an actor's soft-processor
- Perform a correlation power analysis attack

FPGAs are powerful...but often prohibitively expensive

This has pushed us towards...

- Cloud-FPGA leasing schemes (temporal sharing)
- Integration of proprietary IP
- Full FPGA virtualization (temporospatial sharing)

Observation: These are all multi-actor structures—potentially running hidden opaque circuitry.

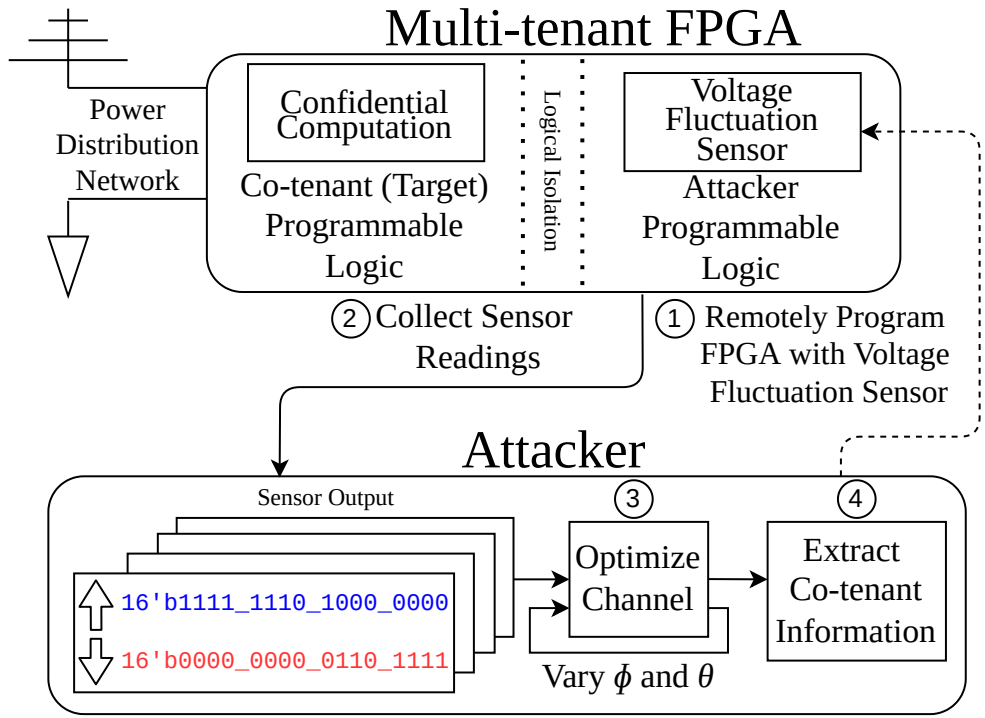
While logical boundaries may be in place, they all share the same power system!

If a dedicated actor were able to instantiate a voltage fluctuation sensor within their allocated logic they could...

- Determine what core other actors are executing
- Determine what is running on an actor's soft-processor
- Perform a correlation power analysis attack
- Detect round 7 of AES to introduce a power fault into the system

Temporospatial (Multi-Tenant) Cloud FPGAs

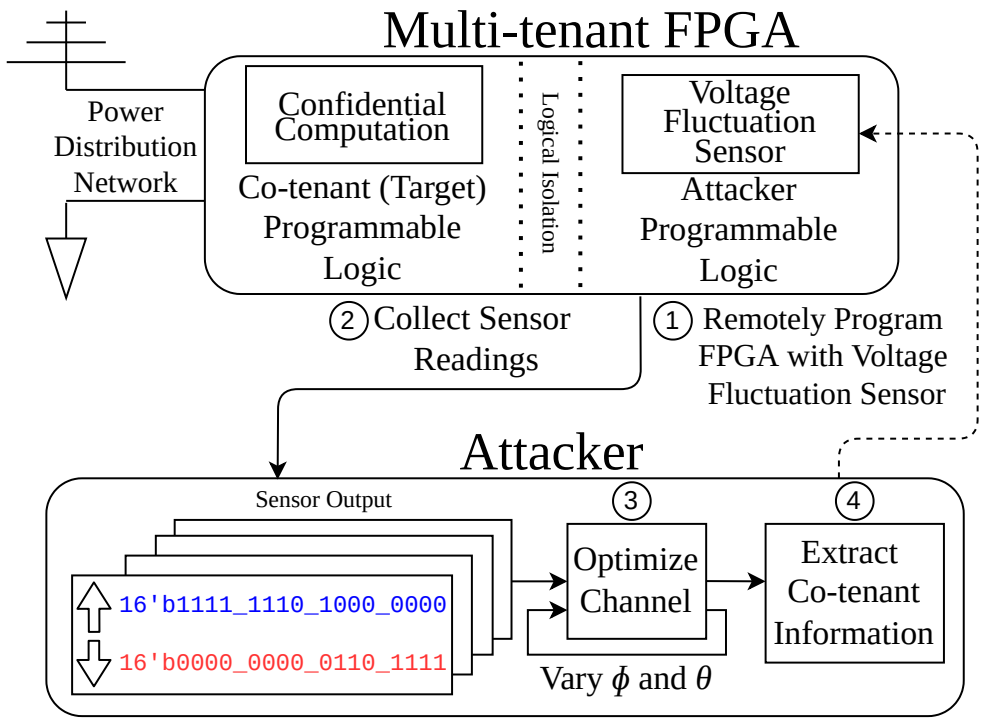
We refine our threat model around cloud multi-tenant FPGAs—but we study fundamental qualities of voltage fluctuation sensors that can apply to any multi-actor structure.



Temporospatial (Multi-Tenant) Cloud FPGAs

We refine our threat model around cloud multi-tenant FPGAs—but we study fundamental qualities of voltage fluctuation sensors that can apply to any multi-actor structure.

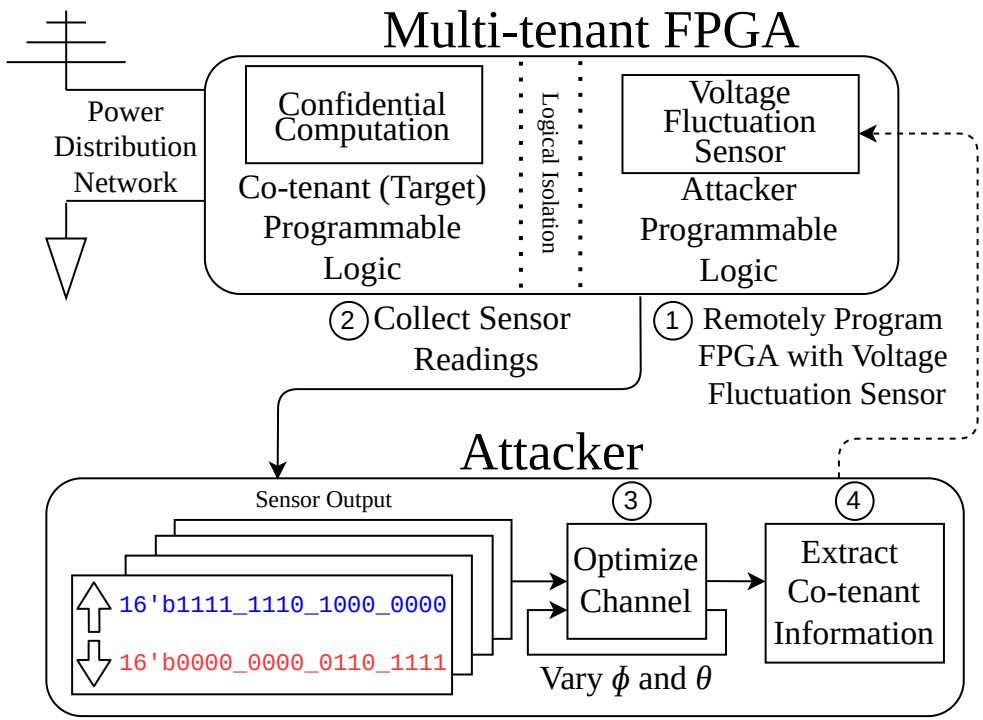
1. Attacker co-locates with another user and deploys voltage sensor



Temporospatial (Multi-Tenant) Cloud FPGAs

We refine our threat model around cloud multi-tenant FPGAs—but we study fundamental qualities of voltage fluctuation sensors that can apply to any multi-actor structure.

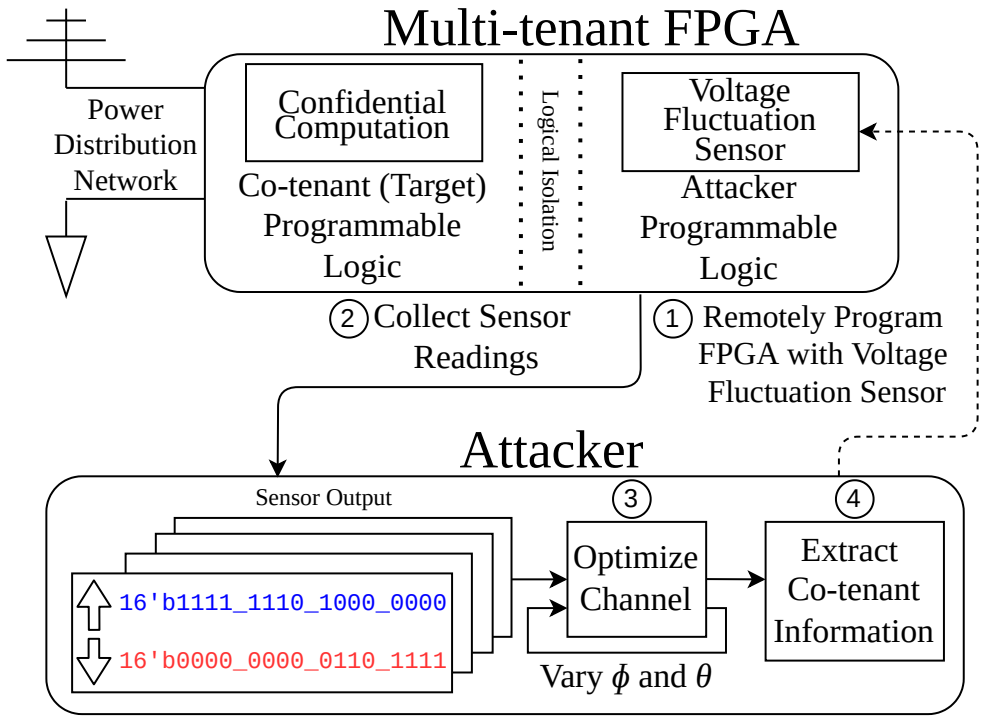
1. Attacker co-locates with another user and deploys voltage sensor
2. Collects sensor readings



Temporospatial (Multi-Tenant) Cloud FPGAs

We refine our threat model around cloud multi-tenant FPGAs—but we study fundamental qualities of voltage fluctuation sensors that can apply to any multi-actor structure.

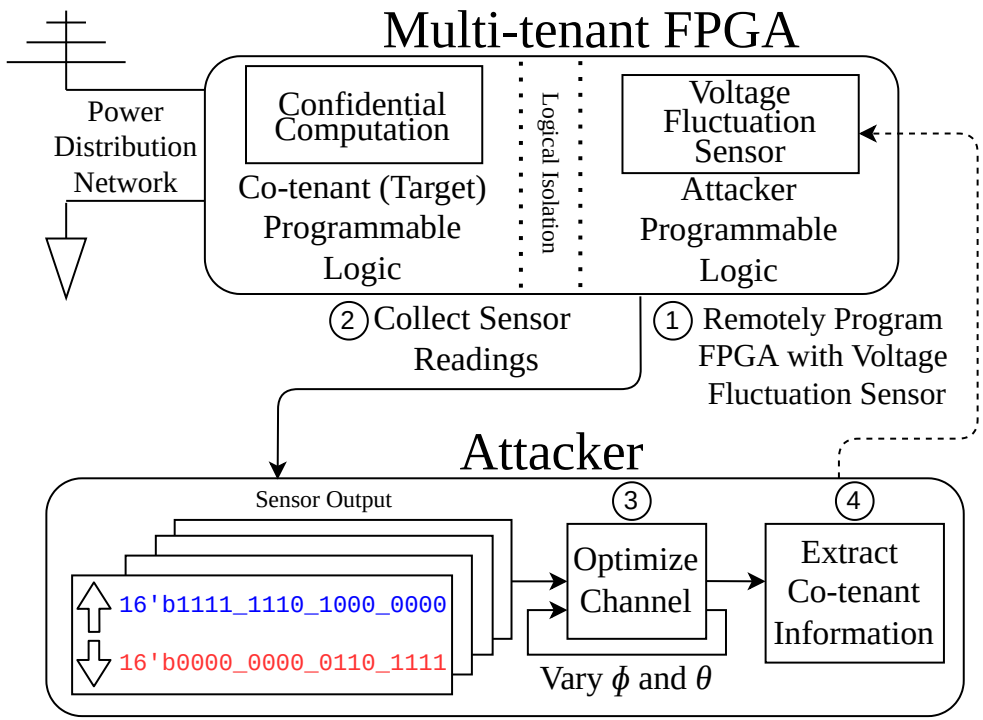
1. Attacker co-locates with another user and deploys voltage sensor
2. Collects sensor readings
3. Optimize and based on readings



Temporospatial (Multi-Tenant) Cloud FPGAs

We refine our threat model around cloud multi-tenant FPGAs—but we study fundamental qualities of voltage fluctuation sensors that can apply to any multi-actor structure.

1. Attacker co-locates with another user and deploys voltage sensor
2. Collects sensor readings
3. Optimize and based on readings
4. Extract data from sensor readings



Voltage Fluctuation Sensors

We are interested in Time-to-Digital Converters (TDC):

Voltage Fluctuation Sensors

We are interested in Time-to-Digital Converters (TDC):

1. An instrument for synchronously measuring the load on the power distribution network

Voltage Fluctuation Sensors

We are interested in Time-to-Digital Converters (TDC):

1. An instrument for synchronously measuring the load on the power distribution network
2. Easy to disguise as they resemble carry-adders and can be designed to include no timing violations

Voltage Fluctuation Sensors

We are interested in Time-to-Digital Converters (TDC):

1. An instrument for synchronously measuring the load on the power distribution network
2. Easy to disguise as they resemble carry-adders and can be designed to include no timing violations

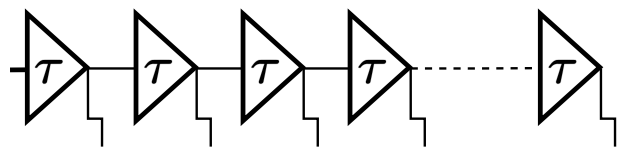
A brief overview of a canonical TDC.

Voltage Fluctuation Sensors

We are interested in Time-to-Digital Converters (TDC):

1. An instrument for synchronously measuring the load on the power distribution network
2. Easy to disguise as they resemble carry-adders and can be designed to include no timing violations

A brief overview of a canonical TDC.



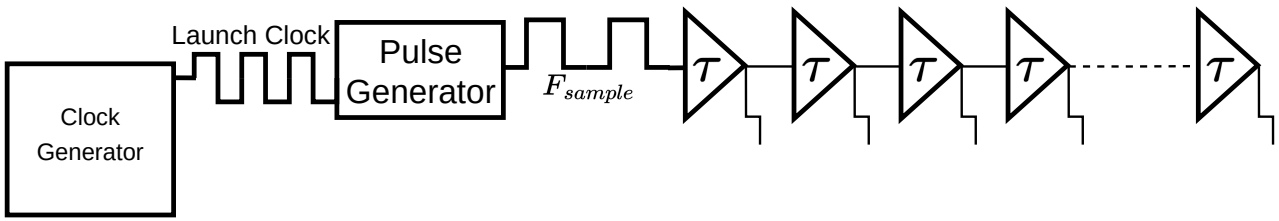
*An array of elements with uniform delay

Voltage Fluctuation Sensors

We are interested in Time-to-Digital Converters (TDC):

1. An instrument for synchronously measuring the load on the power distribution network
2. Easy to disguise as they resemble carry-adders and can be designed to include no timing violations

A brief overview of a canonical TDC.



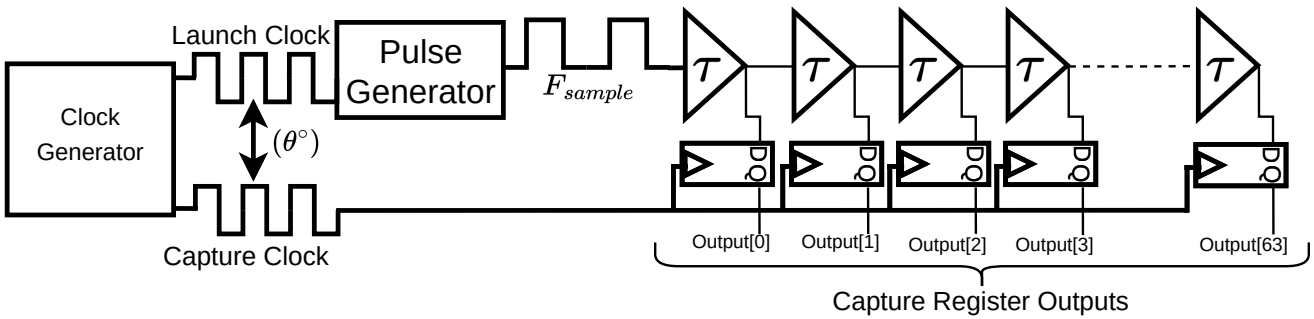
*Launch clock sends rising/falling pulses through delay elements

Voltage Fluctuation Sensors

We are interested in Time-to-Digital Converters (TDC):

1. An instrument for synchronously measuring the load on the power distribution network
2. Easy to disguise as they resemble carry-adders and can be designed to include no timing violations

A brief overview of a canonical TDC.



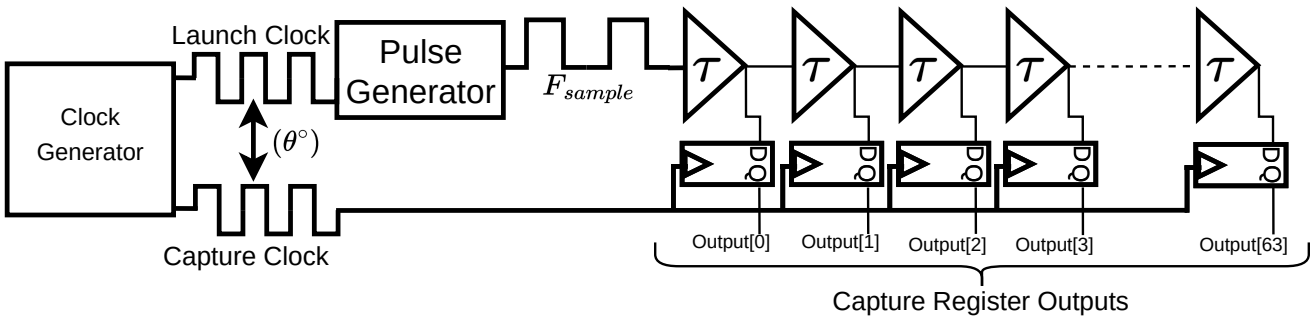
*Capture clock, which is phase offset a constant value from the launch, captures how far signals propagated through delay elements

Voltage Fluctuation Sensors

We are interested in Time-to-Digital Converters (TDC):

1. An instrument for synchronously measuring the load on the power distribution network
2. Easy to disguise as they resemble carry-adders and can be designed to include no timing violations

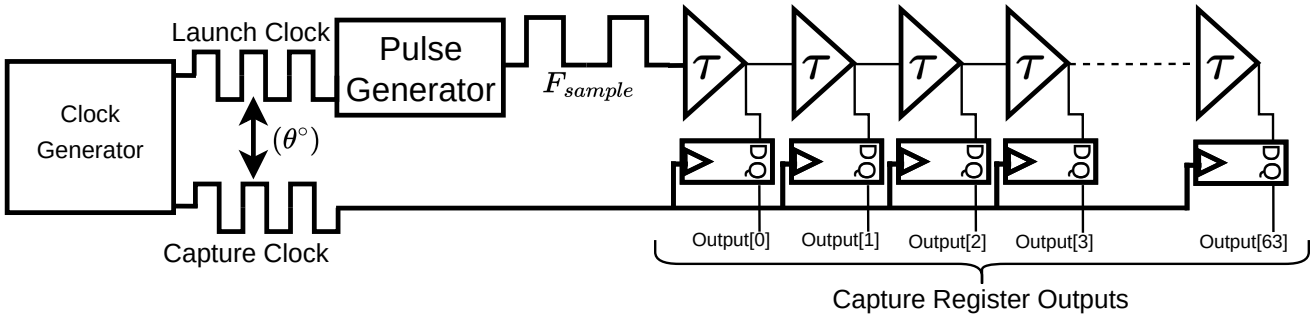
A brief overview of a canonical TDC.



Capture output distance $\propto$ state of the PDN

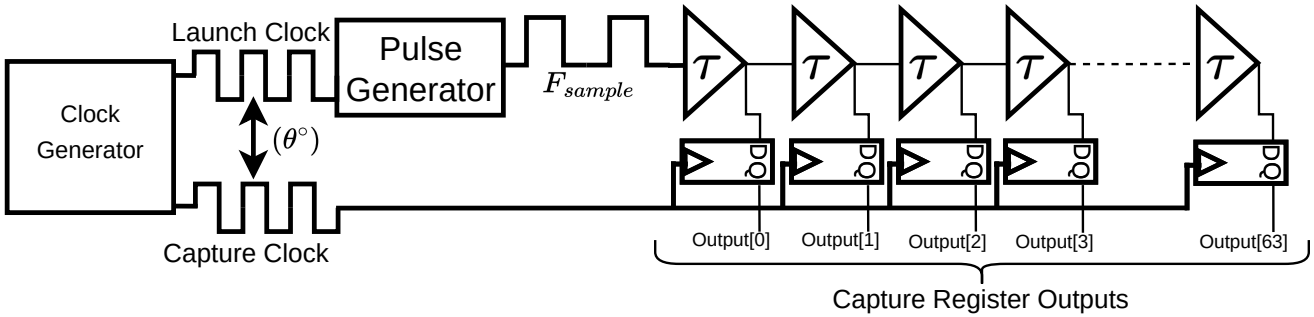
Known Problems: Architectural Irregularities

This is a nice theoretical model:



Known Problems: Architectural Irregularities

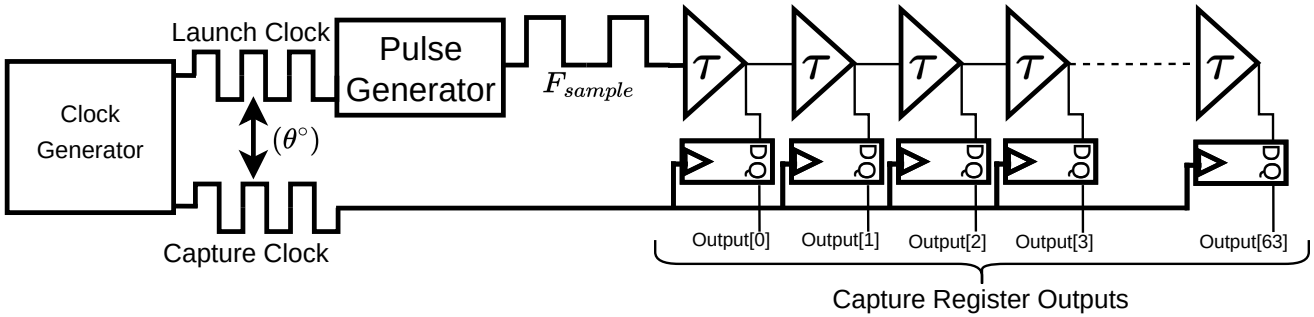
This is a nice theoretical model:



Perfect delay line doesn't exist:

Known Problems: Architectural Irregularities

This is a nice theoretical model:

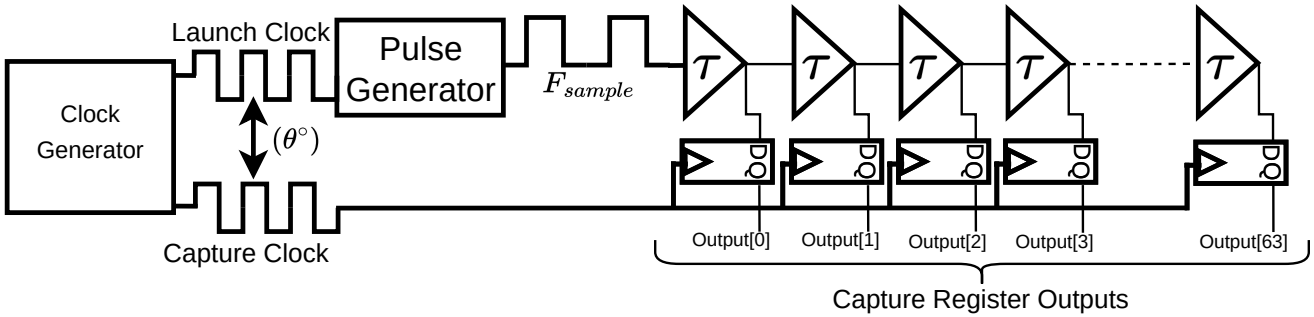


Perfect delay line doesn't exist:

- More linear propagation = more responsive to fluctuations

Known Problems: Architectural Irregularities

This is a nice theoretical model:



Perfect delay line doesn't exist:

- More linear propagation = more responsive to fluctuations
- Faster propagation = higher resolution

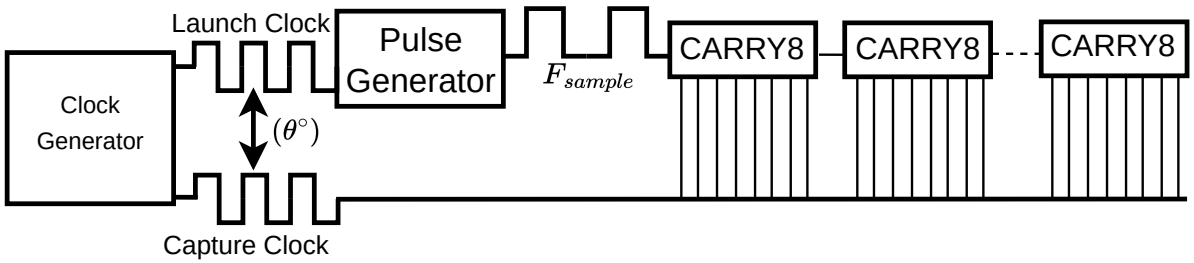
Known Problems: Architectural Irregularities

Known Problems: Architectural Irregularities

Map TDC to CARRY primitives. Fast and linear....locally.

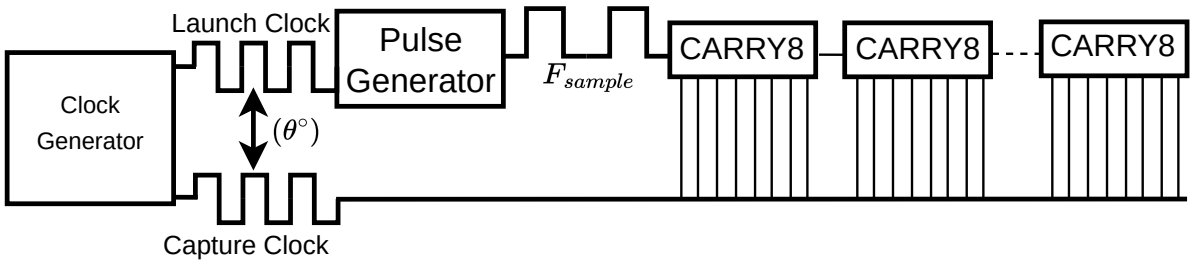
Known Problems: Architectural Irregularities

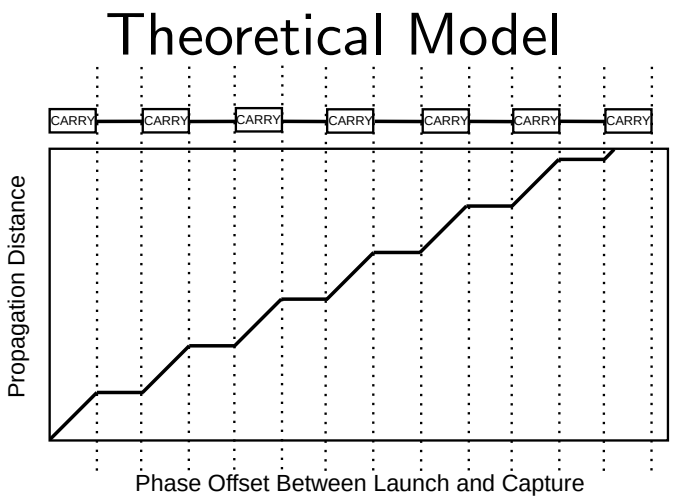
Map TDC to CARRY primitives. Fast and linear....locally.



Known Problems: Architectural Irregularities

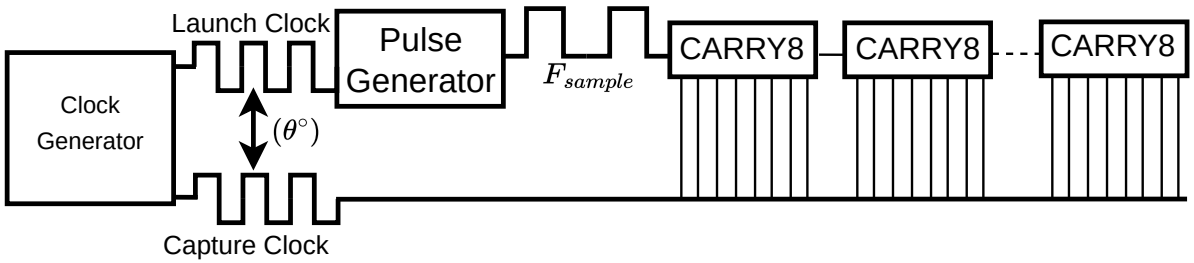
Map TDC to CARRY primitives. Fast and linear....locally.



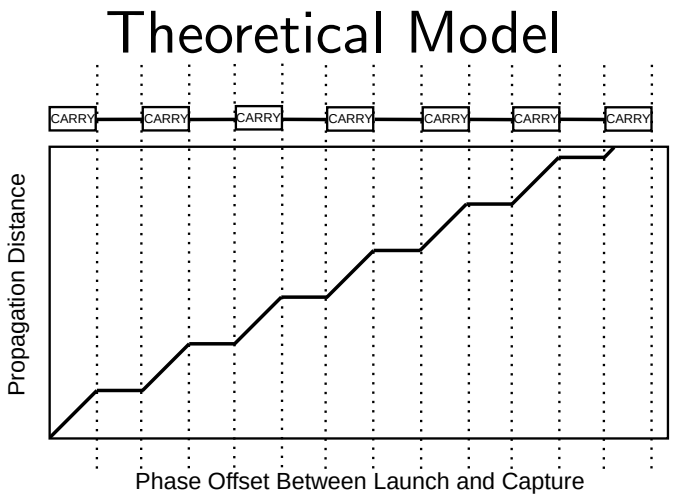


Known Problems: Architectural Irregularities

Map TDC to CARRY primitives. Fast and linear....locally.

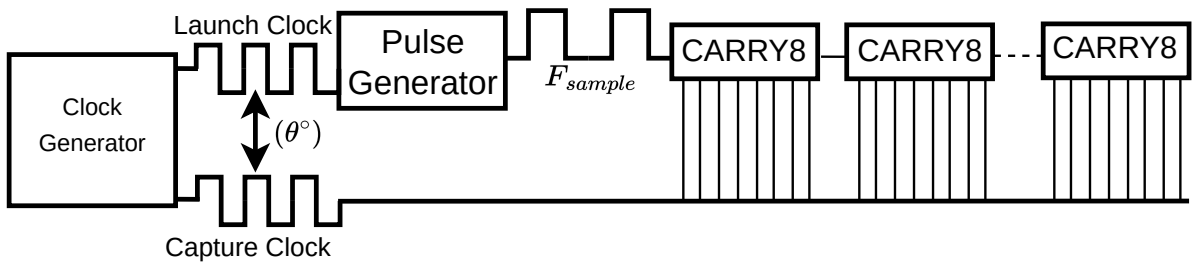


The data bears this out. Linear 4 bits on PYNQ (CARRY4s), linear 8 bits on AWS (CARRY8s).



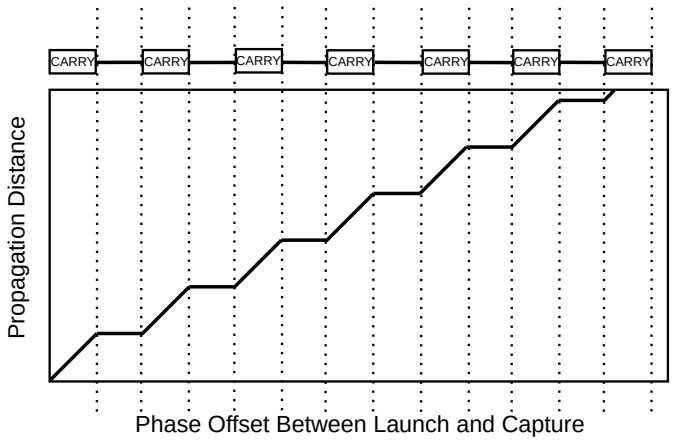
Known Problems: Architectural Irregularities

Map TDC to CARRY primitives. Fast and linear....locally.

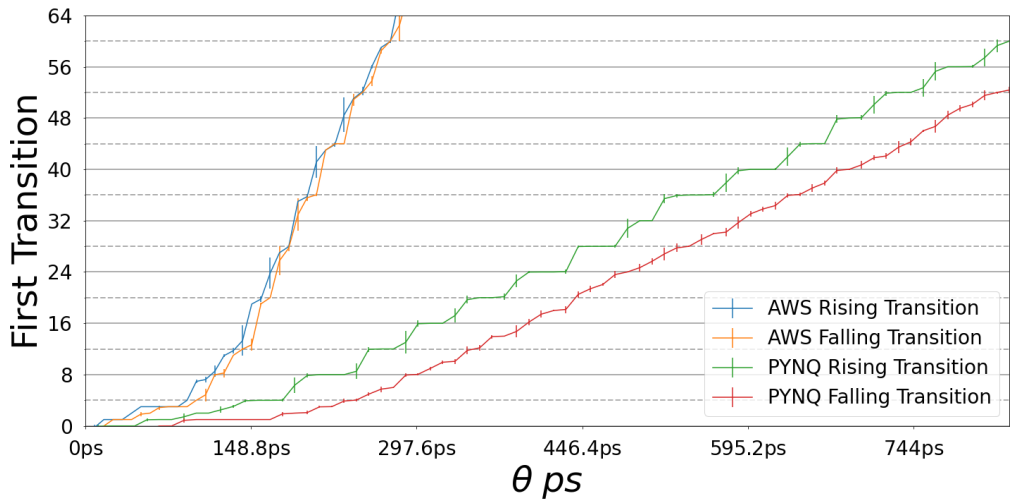


The data bears this out. Linear 4 bits on PYNQ (CARRY4s), linear 8 bits on AWS (CARRY8s).

Theoretical Model

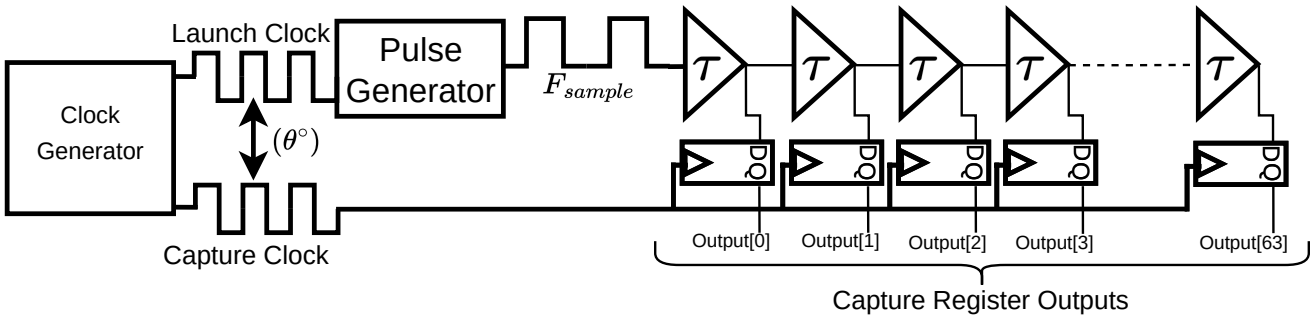


Physical Validation



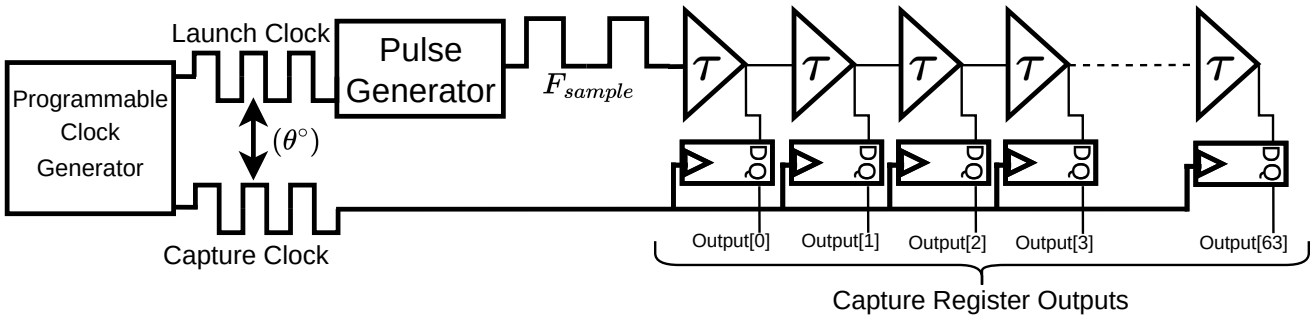
Solution: Dynamic Tuning

Constant phase offset.



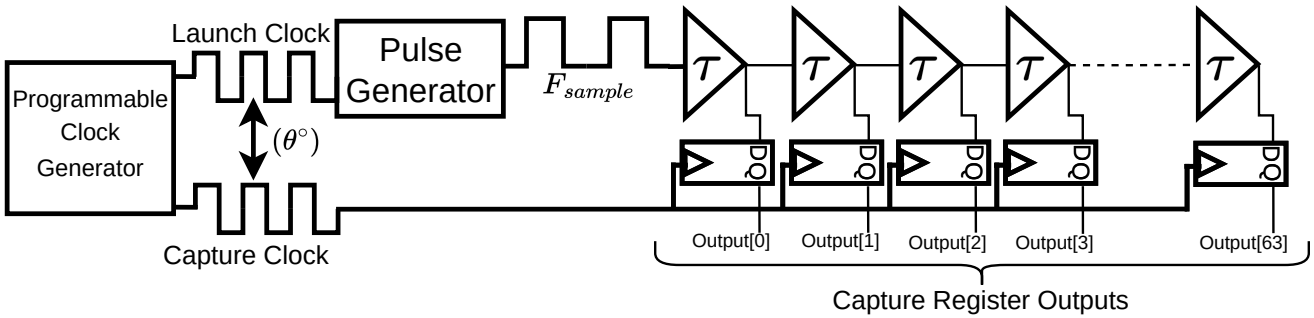
Solution: Dynamic Tuning

Dynamic phase offset.



Solution: Dynamic Tuning

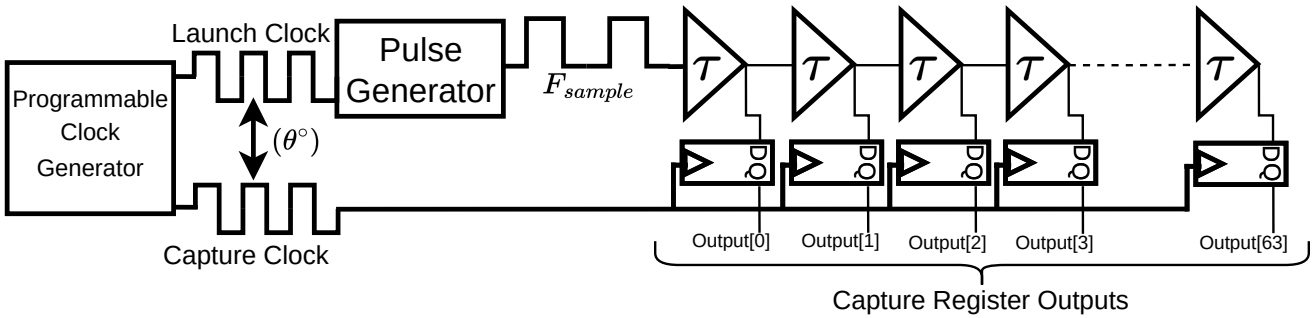
Dynamic phase offset.



- Leverage programmable clock generator

Solution: Dynamic Tuning

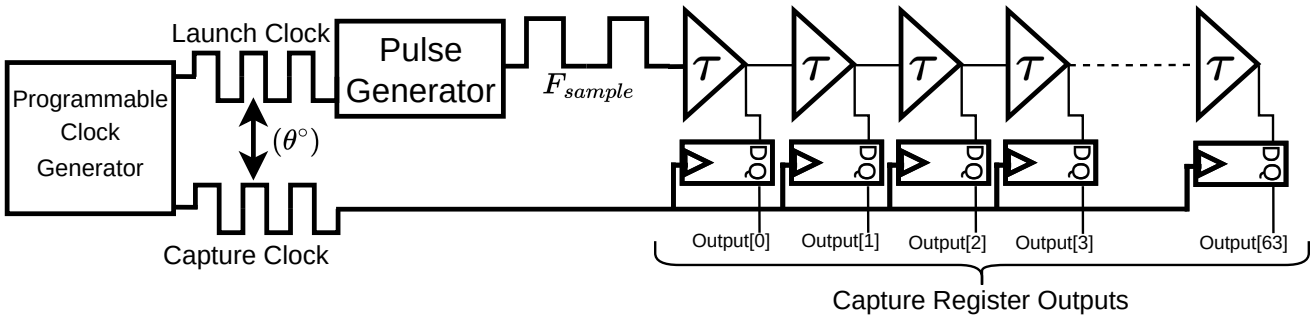
Dynamic phase offset.



- Leverage programmable clock generator
- Propagation distance is now configurable

Solution: Dynamic Tuning

Dynamic phase offset.



- Leverage programmable clock generator
- Propagation distance is now configurable
- Attacker can place transition at ideal point within CARRY primitive, improving sensor response to power fluctuations.

A New Problem: Sampling Phase Alignment

- , the phase relationship between launch and capture defines a **window**

A New Problem: Sampling Phase Alignment

- , the phase relationship between launch and capture defines a **window**
- Only power fluctuations within window are captured by the TDC

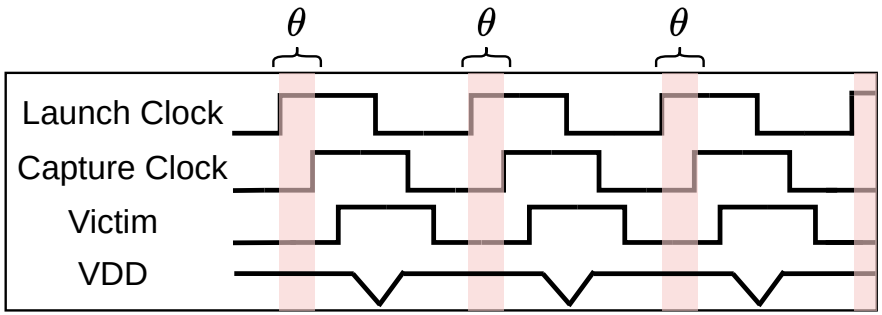
A New Problem: Sampling Phase Alignment

- , the phase relationship between launch and capture defines a **window**
- Only power fluctuations within window are captured by the TDC
- Victim core is also likely synchronous, and induced power fluctuation is brief

A New Problem: Sampling Phase Alignment

- , the phase relationship between launch and capture defines a **window**
- Only power fluctuations within window are captured by the TDC
- Victim core is also likely synchronous, and induced power fluctuation is brief

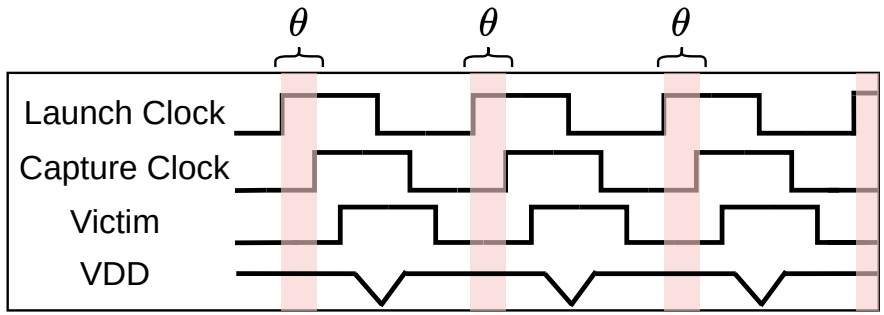
Bad Phase ( ) Alignment!



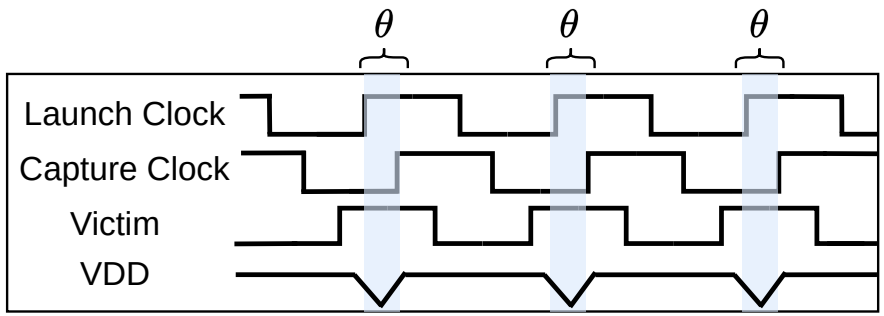
A New Problem: Sampling Phase Alignment

- , the phase relationship between launch and capture defines a **window**
- Only power fluctuations within window are captured by the TDC
- Victim core is also likely synchronous, and induced power fluctuation is brief

Bad Phase ( ) Alignment!



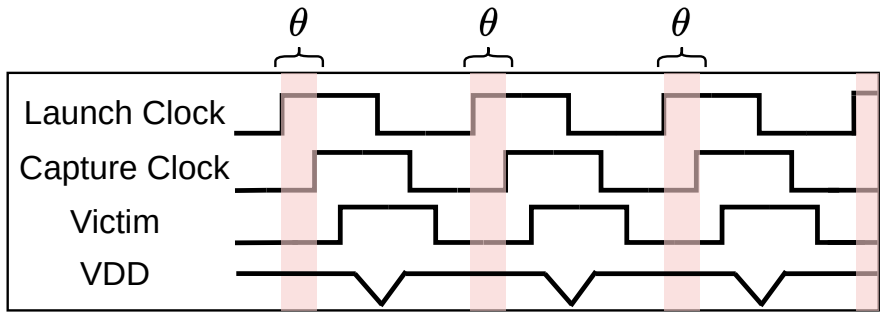
Good Phase ( ) Alignment!



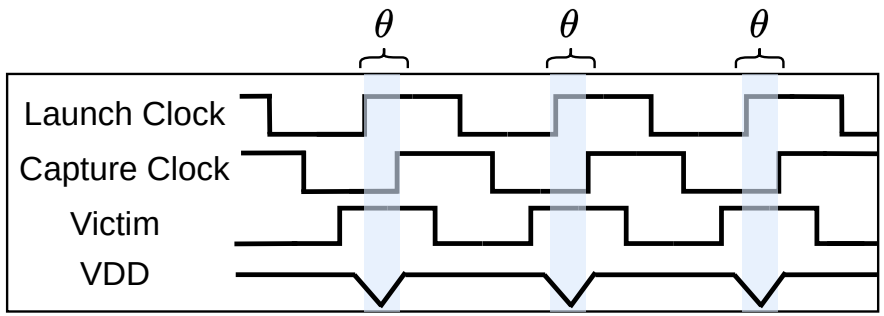
A New Problem: Sampling Phase Alignment

- , the phase relationship between launch and capture defines a **window**
- Only power fluctuations within window are captured by the TDC
- Victim core is also likely synchronous, and induced power fluctuation is brief
- Lets phase shift launch and capture clock together, wrt victim computation

Bad Phase ( ) Alignment!

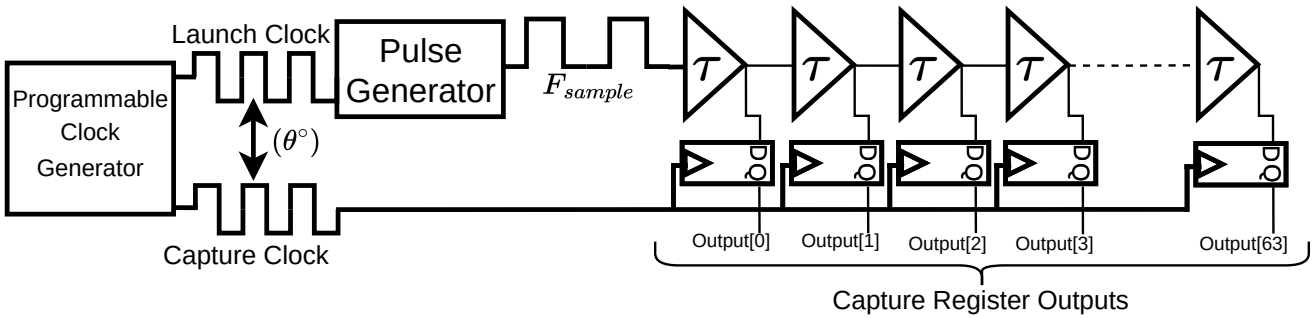


Good Phase ( ) Alignment!



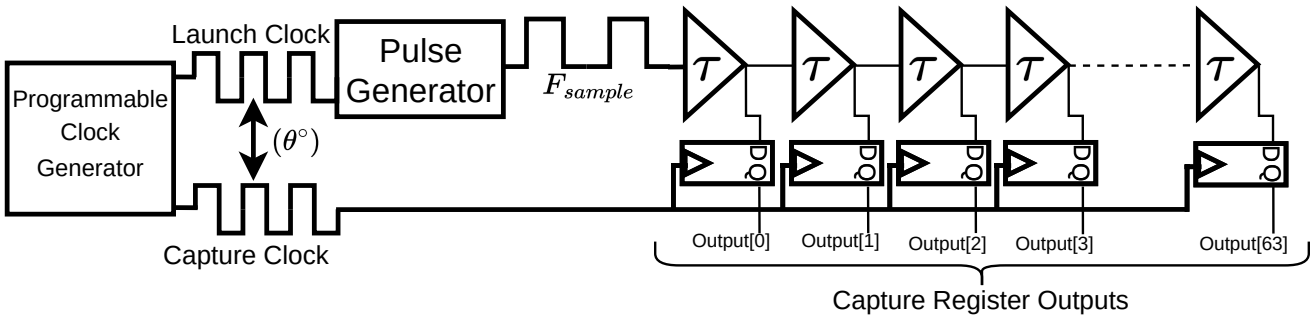
Solution: Dynamic Co-Tenant Phase Alignment

Our tunable Time-to-Digital Converter:

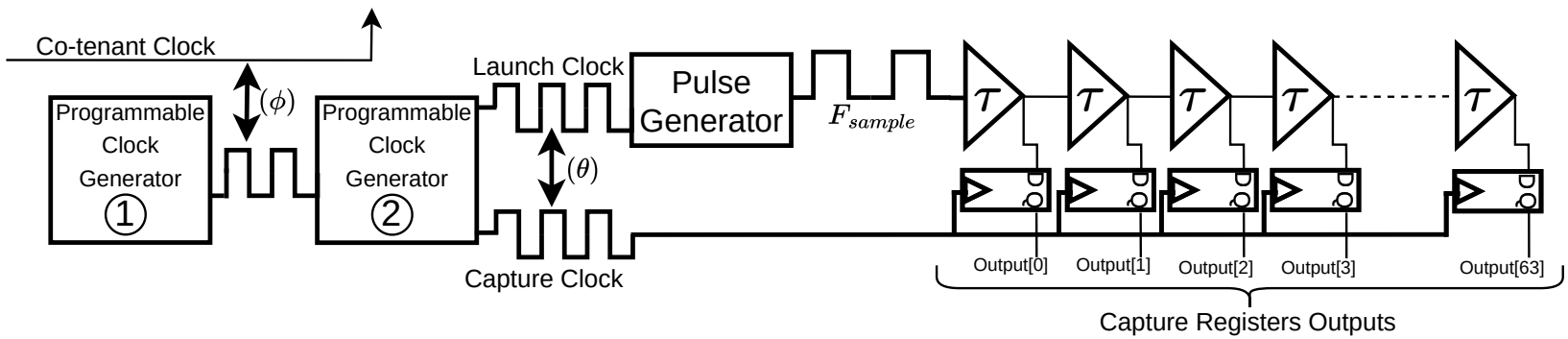


Solution: Dynamic Co-Tenant Phase Alignment

Our tunable Time-to-Digital Converter:



Our and tunable Time-to-Digital Converter:



Solution: Dynamic Co-Tenant Phase Alignment

- Instantiate sensor alongside soft-processor AES. Both 25MHz.

Solution: Dynamic Co-Tenant Phase Alignment

- Instantiate sensor alongside soft-processor AES. Both 25MHz.
- Rotate by two periods with processor disabled and measure.

Solution: Dynamic Co-Tenant Phase Alignment

- Instantiate sensor alongside soft-processor AES. Both 25MHz.
- Rotate by two periods with processor disabled and measure.
- Rotate by two periods with processor enabled and measure.

Solution: Dynamic Co-Tenant Phase Alignment

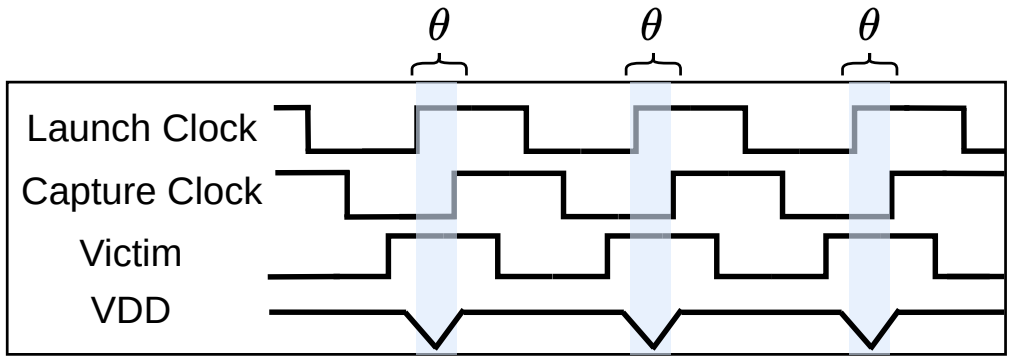
- Instantiate sensor alongside soft-processor AES. Both 25MHz.
- Rotate by two periods with processor disabled and measure.
- Rotate by two periods with processor enabled and measure.

Expect to see a single optimal

Solution: Dynamic Co-Tenant Phase Alignment

- Instantiate sensor alongside soft-processor AES. Both 25MHz.
- Rotate by two periods with processor disabled and measure.
- Rotate by two periods with processor enabled and measure.

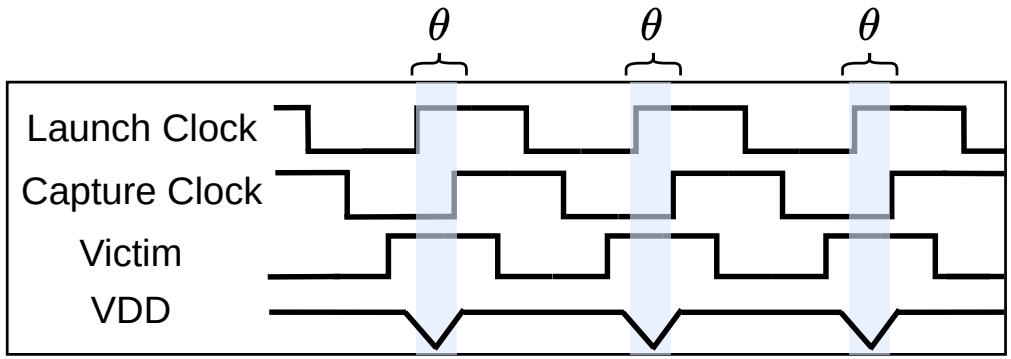
Expect to see a single optimal



Solution: Dynamic Co-Tenant Phase Alignment

- Instantiate sensor alongside soft-processor AES. Both 25MHz.
- Rotate by two periods with processor disabled and measure.
- Rotate by two periods with processor enabled and measure.

Expect to see a single optimal

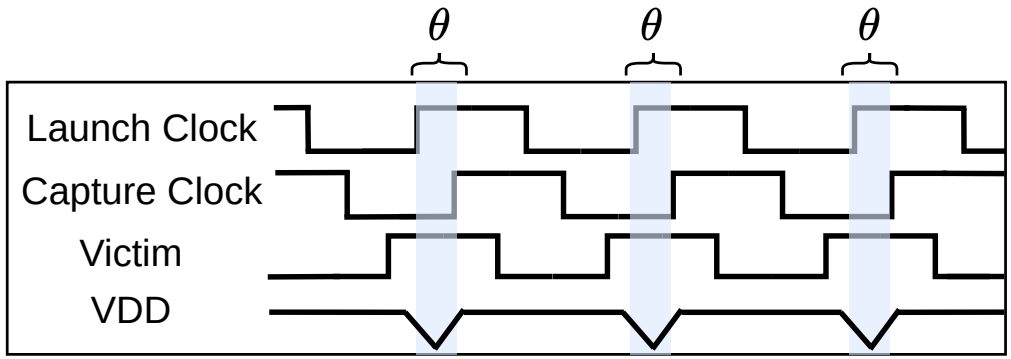


Many "optimal"

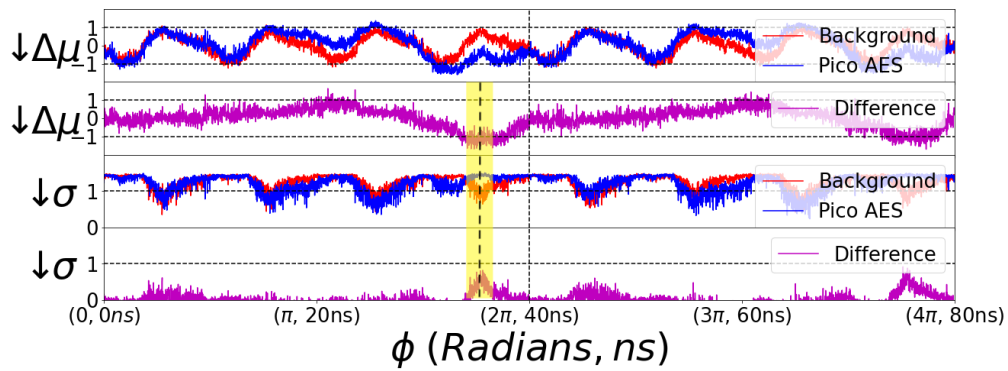
Solution: Dynamic Co-Tenant Phase Alignment

- Instantiate sensor alongside soft-processor AES. Both 25MHz.
- Rotate by two periods with processor disabled and measure.
- Rotate by two periods with processor enabled and measure.

Expect to see a single optimal



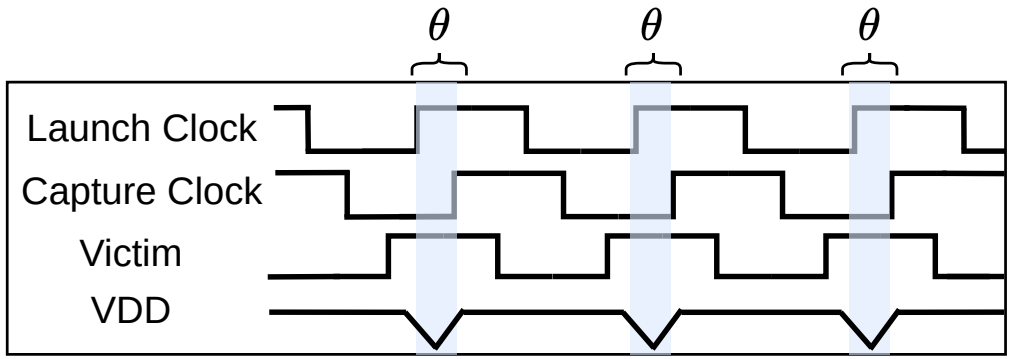
Many "optimal"



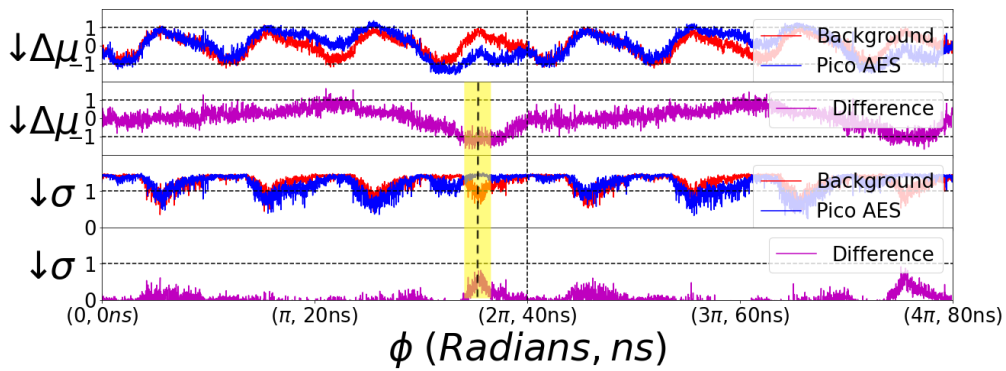
Solution: Dynamic Co-Tenant Phase Alignment

- Instantiate sensor alongside soft-processor AES. Both 25MHz.
- Rotate by two periods with processor disabled and measure.
- Rotate by two periods with processor enabled and measure.
- Background sweep varies by

Expect to see a single optimal



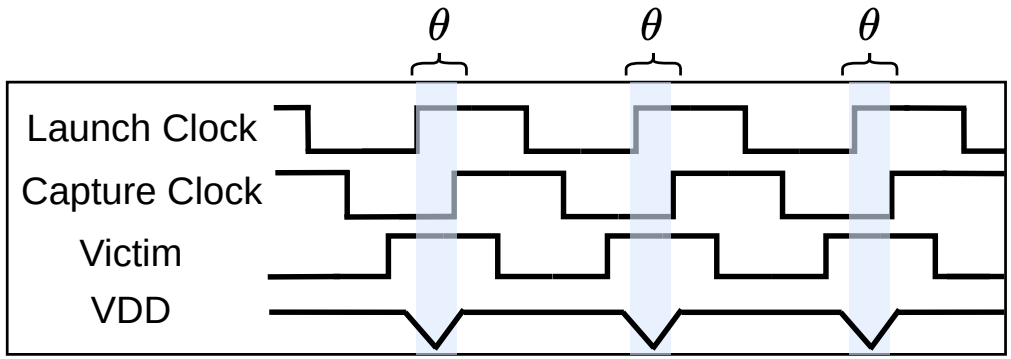
Many "optimal"



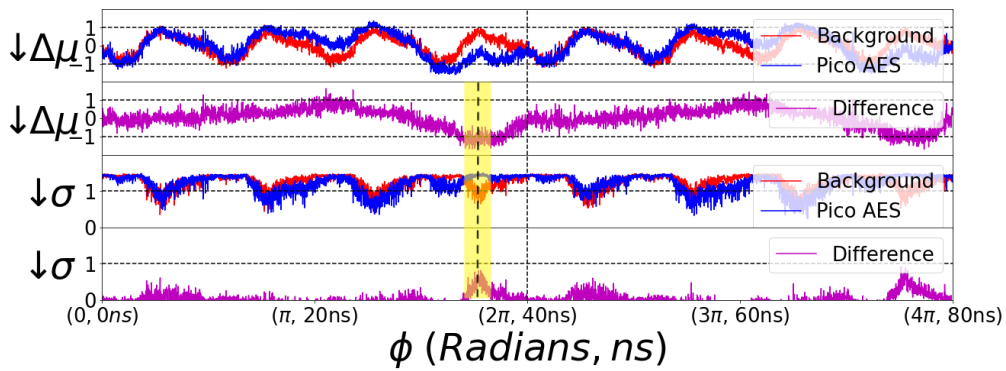
Solution: Dynamic Co-Tenant Phase Alignment

- Instantiate sensor alongside soft-processor AES. Both 25MHz.
- Rotate by two periods with processor disabled and measure.
- Rotate by two periods with processor enabled and measure.
- Background sweep varies by
- Optimal blends into sensor background noise

Expect to see a single optimal



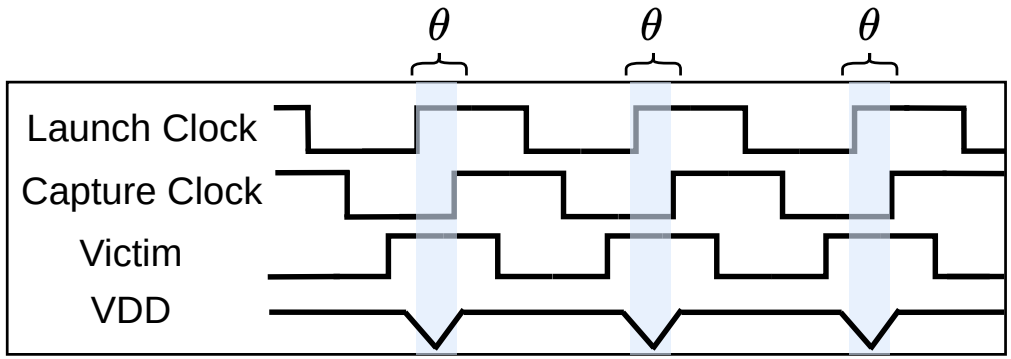
Many "optimal"



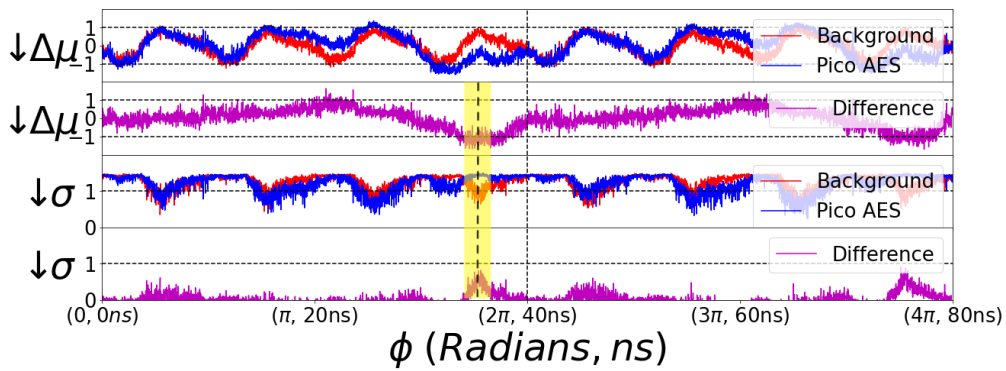
Solution: Dynamic Co-Tenant Phase Alignment

- Instantiate sensor alongside soft-processor AES. Both 25MHz.
- Rotate by two periods with processor disabled and measure.
- Rotate by two periods with processor enabled and measure.
- Background sweep varies by
- Optimal blends into sensor background noise

Expect to see a single optimal



Many "optimal"



Taking the di erence from the background exposes optimal to capture power uctuations induced by victim.

Classification Attack

- Sensor co-located with each of 13 victim computations on multiple boards

Classification Attack

- Sensor co-located with each of 13 victim computations on multiple boards
- Sensor is tuned to some value of and to minimize (maximize) and

Classification Attack

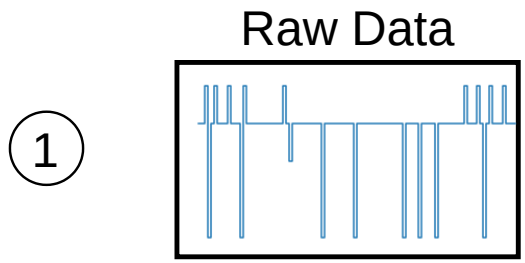
- Sensor co-located with each of 13 victim computations on multiple boards
- Sensor is tuned to some value of and to minimize (maximize) and
- Sensor is sampled as victim executes

Classification Attack

- Sensor co-located with each of 13 victim computations on multiple boards
- Sensor is tuned to some value of and to minimize (maximize) and
- Sensor is sampled as victim executes
- Some number of boards are reserved for training, some for testing, representing the hypothetical divide between cloud and local FPGAs.

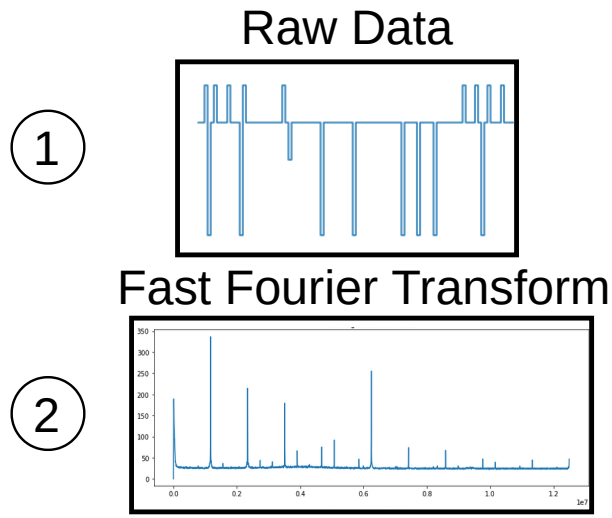
Classification Attack

- Sensor co-located with each of 13 victim computations on multiple boards
- Sensor is tuned to some value of and to minimize (maximize) and
- Sensor is sampled as victim executes
- Some number of boards are reserved for training, some for testing, representing the hypothetical divide between cloud and local FPGAs.
- The data is then processed....



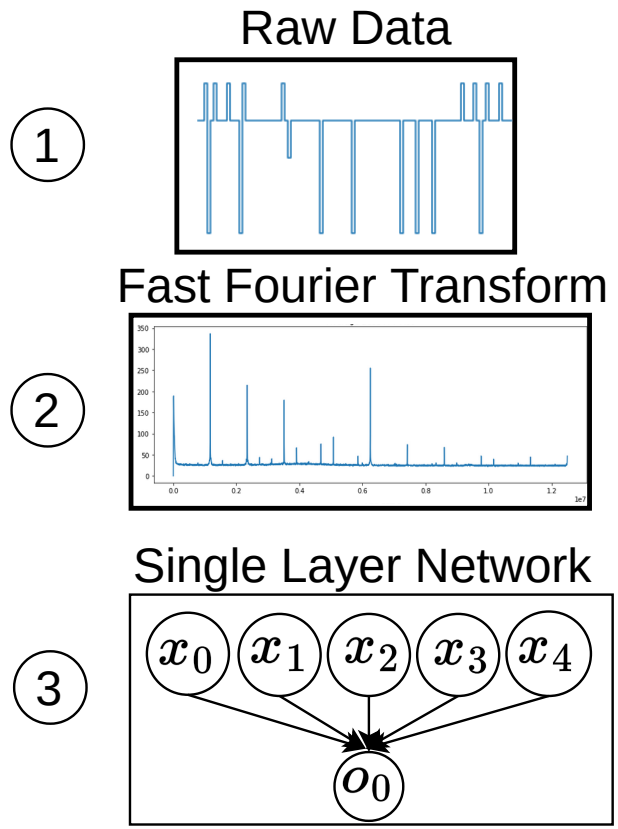
Classification Attack

- Sensor co-located with each of 13 victim computations on multiple boards
- Sensor is tuned to some value of and to minimize (maximize) and
- Sensor is sampled as victim executes
- Some number of boards are reserved for training, some for testing, representing the hypothetical divide between cloud and local FPGAs.
- The data is then processed....



Classification Attack

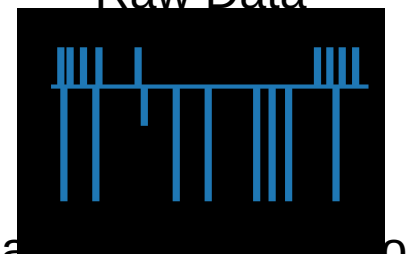
- Sensor co-located with each of 13 victim computations on multiple boards
- Sensor is tuned to some value of and to minimize (maximize) and
- Sensor is sampled as victim executes
- Some number of boards are reserved for training, some for testing, representing the hypothetical divide between cloud and local FPGAs.
- The data is then processed....



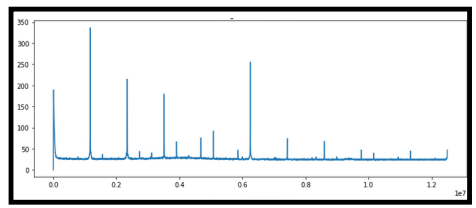
Classification Attack

- Sensor co-located with each of 13 victim computations on multiple boards
- Sensor is tuned to some value of and to minimize (maximize) and
- Sensor is sampled as victim executes
- Some number of boards are reserved for training, some for testing, representing the hypothetical divide between cloud and local FPGAs.
- The data is then processed....

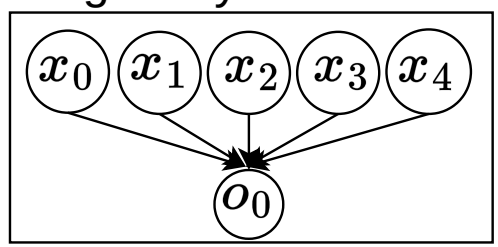
1



2



3



4

Classi cation Attack

- Sensor co-located with each of 13 victim computations on multiple boards
- Sensor is tuned to some value ofand to minimize (maximize) and
- Sensor is sampled as victim executes
- Some number of boards are reserved for training, some for testing, representing the hypothetical divide between cloud and local FPGAs.
- The data is then processed....
- Classi cation accuracy across 13 applications re ects the sensors ability to capture sensitive information across the channel.

Classi cation Accuracy by Tuning Con guration

- Worst case: min standard deviation of (likely a plateau), and (likely phase misaligned).

Classi cation Accuracy by Tuning Con guration

- Worst case: min standard deviation of (likely a plateau), and (likely phase misaligned).

Worst Case: 32.146%

Classi cation Accuracy by Tuning Con guration

- Worst case: min standard deviation of (likely a plateau), and (likely phase misaligned).
- Good : max standard deviation of , and min .

Worst Case: 32.146%

Classi cation Accuracy by Tuning Con guration

- Worst case: min standard deviation of (likely a plateau), and (likely phase misaligned).
- Good : max standard deviation of , and min .

Good : 51.160%

Classi cation Accuracy by Tuning Con guration

- Worst case: min standard deviation of (likely a plateau), and (likely phase misaligned).
- Good : max standard deviation of , and min .
- Good and : max standard deviation of , and max .

Good : 51.160%

Classi cation Accuracy by Tuning Con guration

- Worst case: min standard deviation of (likely a plateau), and (likely phase misaligned).
- Good : max standard deviation of , and min .
- Good and : max standard deviation of , and max .

Good and : 75.788%

Classi cation Accuracy by Tuning Con guration

- Worst case: min standard deviation of (likely a plateau), and (likely phase misaligned).
- Good : max standard deviation of , and min .
- Good and : max standard deviation of , and max .
- Good and : with background subtraction.

Good and : 75.788%

Classi cation Accuracy by Tuning Con guration

- Worst case: min standard deviation of (likely a plateau), and (likely phase misaligned).
- Good : max standard deviation of , and min .
- Good and : max standard deviation of , and max .
- Good and : with background subtraction.

Good and with bg: 75.552%

So background subtraction is useless?

Check the cross validation performance

So background subtraction is useless?

Check the cross validation performance

- Test every combination
  and number of training and
  testing board

So background subtraction is useless?

Check the cross validation performance

- Test every combination and number of training and testing board
- Examine accuracy vs # training boards. Reduces IQR by 2.3X.

So background subtraction is useless?

Check the cross validation performance

- Test every combination and number of training and testing board
- Examine accuracy vs # training boards. Reduces IQR by 2.3X.
- Examine loss vs # training boards. Reduces IQR by 5.8X.

So background subtraction is useless?

Check the cross validation performance

- Test every combination and number of training and testing board
- Examine accuracy vs # training boards. Reduces IQR by 2.3X.
- Examine loss vs # training boards. Reduces IQR by 5.8X.
- Data generalizes better

So background subtraction is useless?

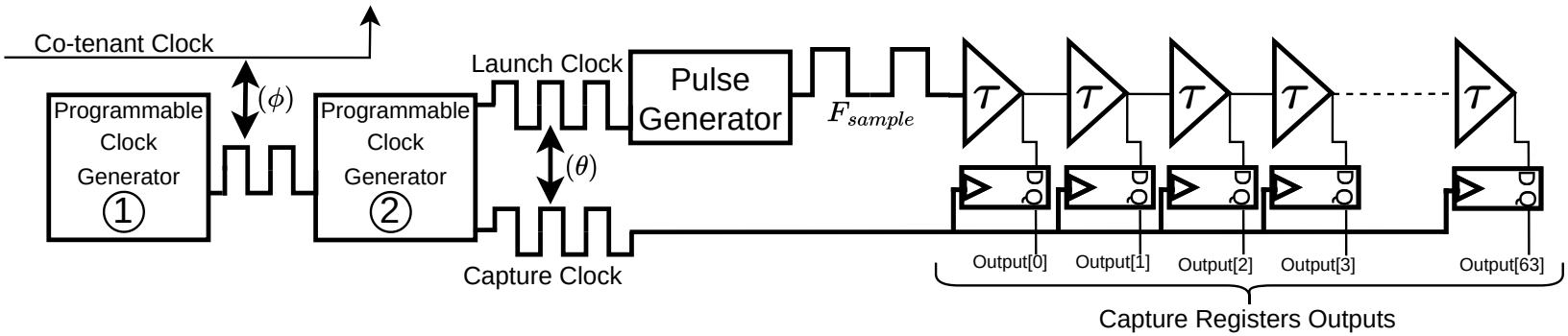
Check the cross validation performance

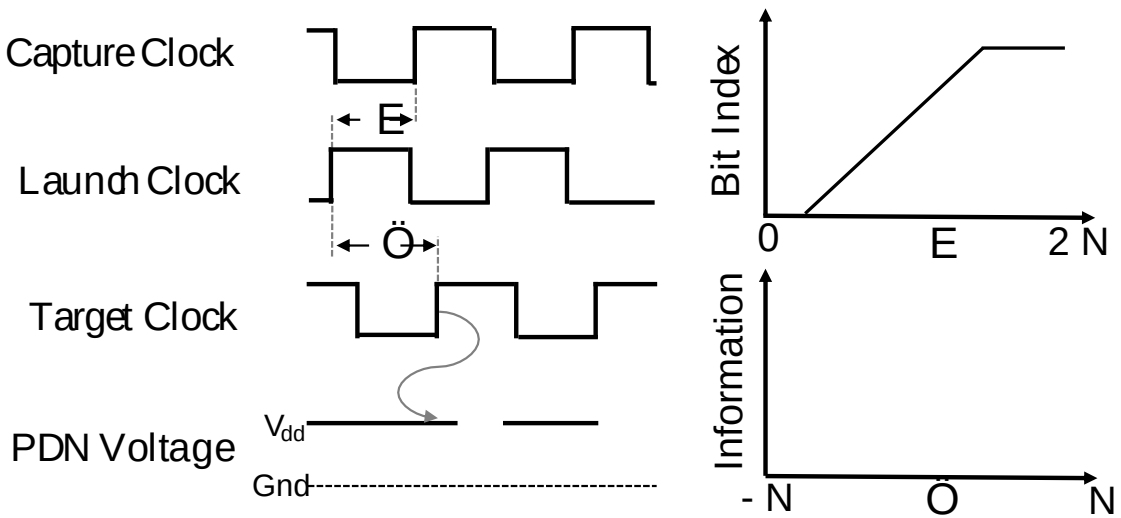
- Test every combination and number of training and testing board
- Examine accuracy vs # training boards. Reduces IQR by 2.3X.
- Examine loss vs # training boards. Reduces IQR by 5.8X.
- Data generalizes better

Background Subtraction is Out-of-Distribution Generalization!

Conclusion/Questions

Don't let and assume a random value!





Thanks!