Pentimento

Data Residue in Digital Hardware

Colin Drewes[1], Olivia Weng[2], Andres Meza[2], Alric Althoff[3], David Kohlbrenner[4], Ryan Kastner[2], and Dustin Richmond[5]

[1]Stanford, [2]UCSD, [3]Cycuity, [4]UW, [5]UCSC

February 12, 2023

An Analogy

Pentimento—The presence or reemergence of early images which have since been painted over.

An Analogy

Pentimento—The presence or reemergence of early images which have since been painted over.

Rembrandt's *An Old Man in Military Costume*

An Analogy

Pentimento—The presence or reemergence of early images which have since been painted over.

Rembrandt's *An Old Man in Military Costume*

X-Ray Imaging

An Analogy

Pentimento—The presence or reemergence of early images which have since been painted over.

Rembrandt's *An Old Man in Military Costume*

X-Ray Imaging

An Analogy

Pentimento—The presence or reemergence of early images which have since been painted over.

Why?

Rembrandt's *An Old Man in Military Costume*

X-Ray Imaging

An Analogy

Pentimento—The presence or reemergence of early images which have since been painted over.

Why?

- Reusing canvases

Rembrandt's *An Old Man in Military Costume*

X-Ray Imaging

An Analogy

Pentimento—The presence or reemergence of early images which have since been painted over.

Why?

- Reusing canvases
- Covering mistakes

Rembrandt's *An Old Man in Military Costume*

X-Ray Imaging

An Analogy

Pentimento—The presence or reemergence of early images which have since been painted over.

Why?

- Reusing canvases
- Covering mistakes
- Censorship

Rembrandt's *An Old Man in Military Costume*

X-Ray Imaging

An Analogy

Pentimento—The presence or reemergence of early images which have since been painted over.

Why?

- Reusing canvases
- Covering mistakes
- Censorship

Digital pentimenti

Rembrandt's *An Old Man in Military Costume*

X-Ray Imaging

An Analogy

Pentimento—The presence or reemergence of early images which have since been painted over.

Why?

- Reusing canvases
- Covering mistakes
- Censorship

Digital pentimenti

- Artifacts of previous data

Rembrandt's *An Old Man in Military Costume*

X-Ray Imaging

An Analogy

Pentimento—The presence or reemergence of early images which have since been painted over.

Why?

- Reusing canvases
- Covering mistakes
- Censorship

Digital pentimenti

- Artifacts of previous data
- Personal information

Rembrandt's *An Old Man in Military Costume*

X-Ray Imaging

An Analogy

Pentimento—The presence or reemergence of early images which have since been painted over.

Why?

- Reusing canvases
- Covering mistakes
- Censorship

Digital pentimenti

- Artifacts of previous data
- Personal information
- Machine learning weights

Rembrandt's *An Old Man in Military Costume*

X-Ray Imaging

An Analogy

Pentimento—The presence or reemergence of early images which have since been painted over.

Why?

- Reusing canvases
- Covering mistakes
- Censorship

Digital pentimenti

- Artifacts of previous data
- Personal information
- Machine learning weights
- Cryptographic keys

Rembrandt's *An Old Man in Military Costume*

X-Ray Imaging

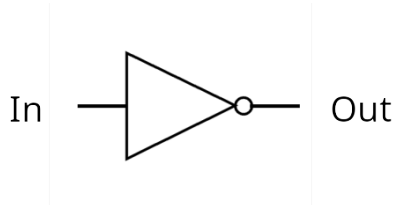
Digital Pentimenti

The reemergence of earlier digital data that has since been overwritten.

Digital Pentimenti

The reemergence of earlier digital data that has since been overwritten.

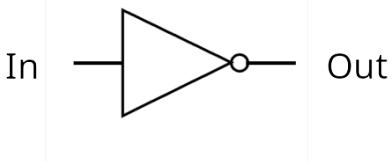
Idealized view of digital logic



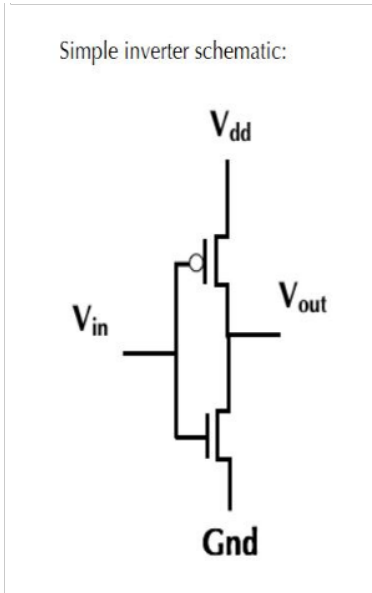
Digital Pentimenti

The reemergence of earlier digital data that has since been overwritten.

Idealized view of digital logic



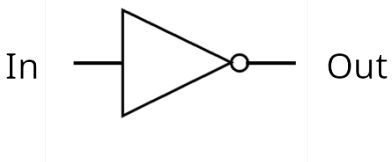
But really...



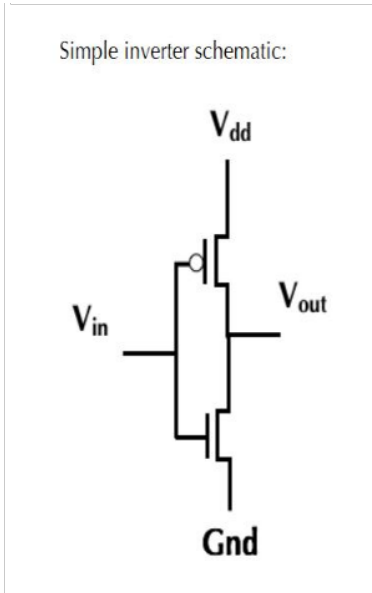
Digital Pentimenti

The reemergence of earlier digital data that has since been overwritten.

Idealized view of digital logic



But really...

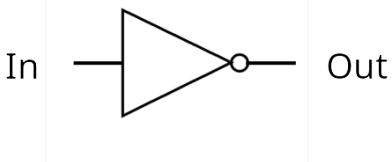


But really...

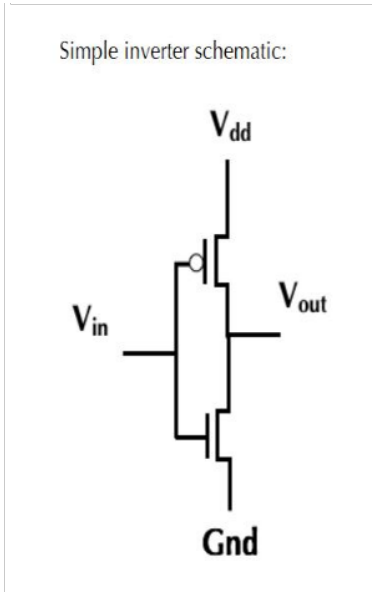
Digital Pentimenti

The reemergence of earlier digital data that has since been overwritten.

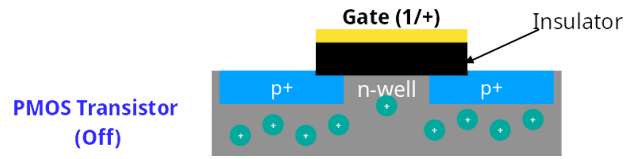
Idealized view of digital logic



But really...



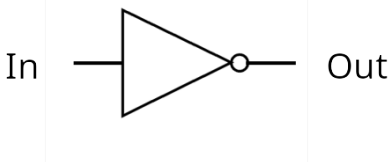
But really...



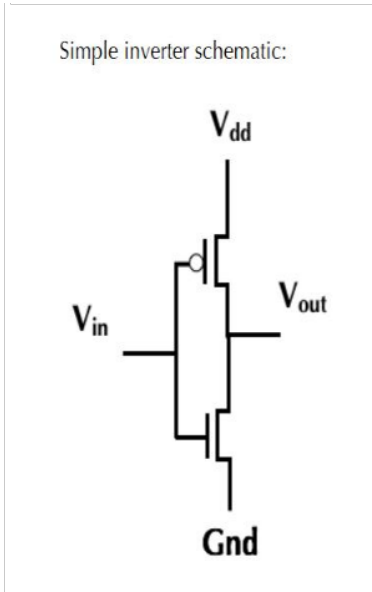
Digital Pentimenti

The reemergence of earlier digital data that has since been overwritten.

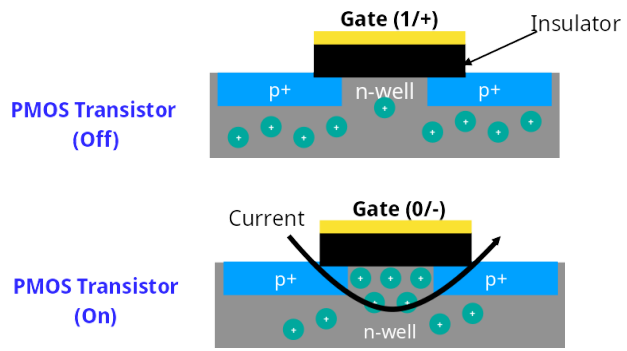
Idealized view of digital logic



But really...



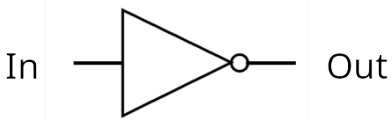
But really...



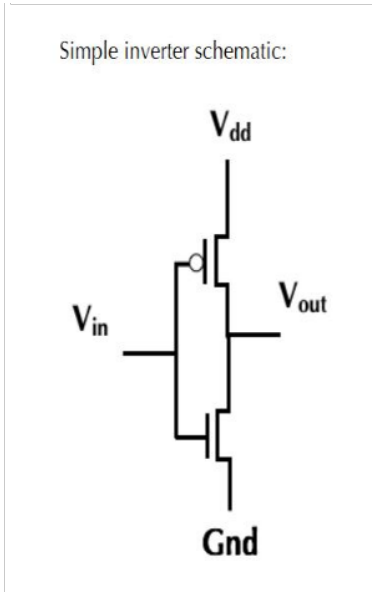
Digital Pentimenti

The reemergence of earlier digital data that has since been overwritten.

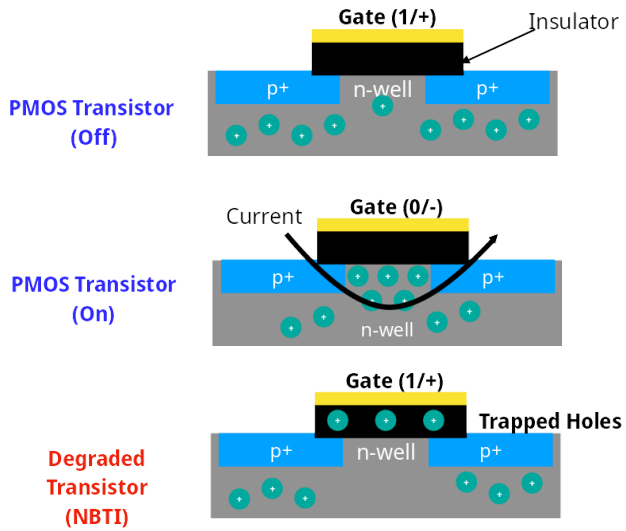
Idealized view of digital logic



But really...

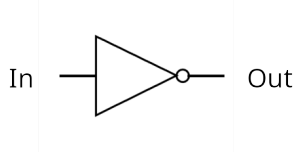


But really...

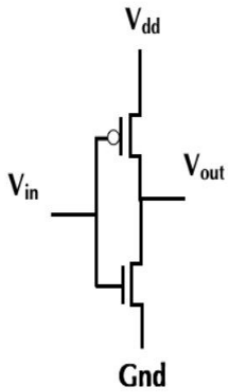


"Negative (-) Bias Temperature Instability"(a Pentimento?)

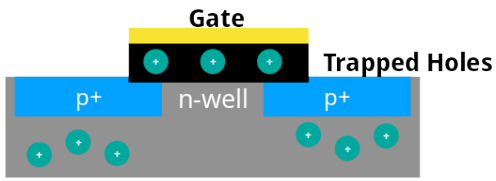
A Pentimenti Emerges



Simple inverter schematic:

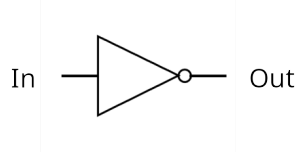


A Pentimenti Emerges

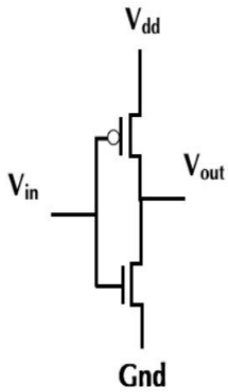


Degraded Transistor (NBTI)

"Negative (-) Bias Temperature Instability"

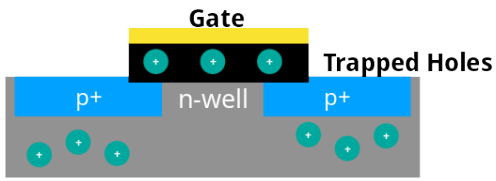


Simple inverter schematic:

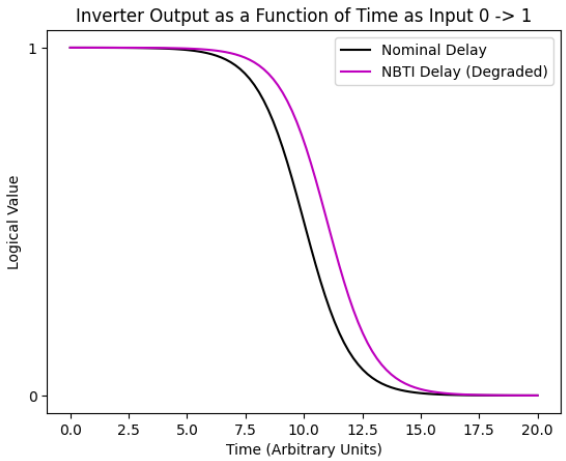


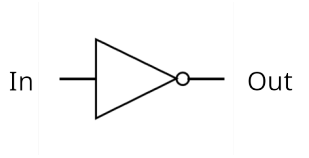
A Pentimenti Emerges

Degraded Transistor (NBTI)

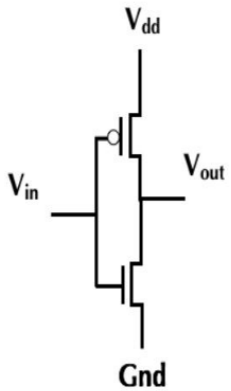


"Negative (-) Bias Temperature Instability"

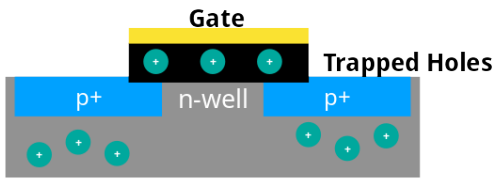




Simple inverter schematic:

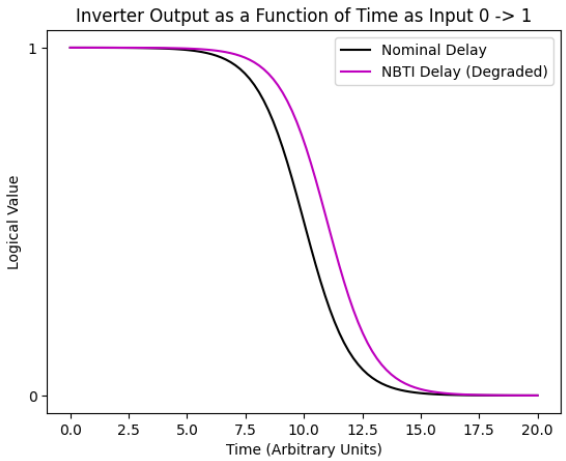


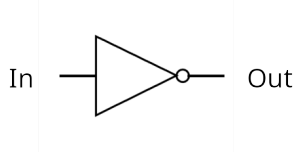
A Pentimenti Emerges

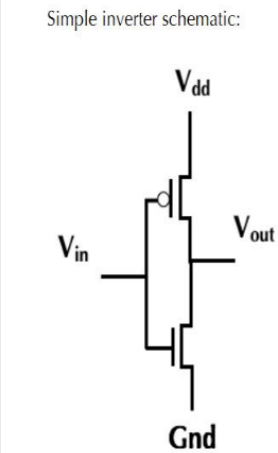


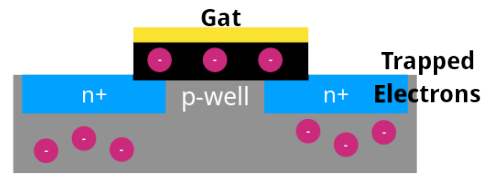
Degraded Transistor (NBTI)

"Negative (-) Bias Temperature Instability"







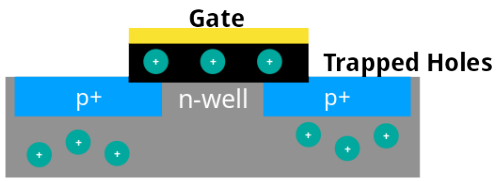


Degraded Transistor (PBTI)

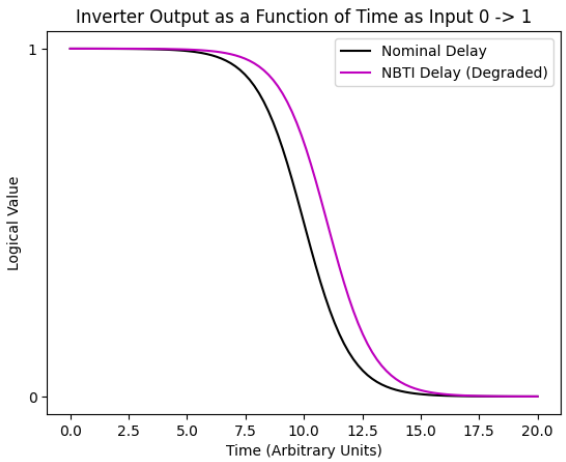
"Positive Bias (+) Temperature Instability"

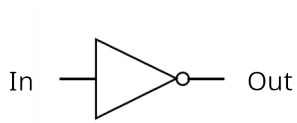
A Pentimenti Emerges

Degraded Transistor (NBTI)

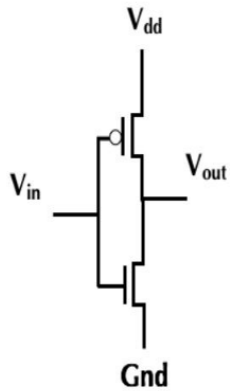


"Negative (-) Bias Temperature Instability"

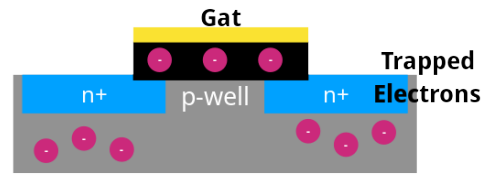




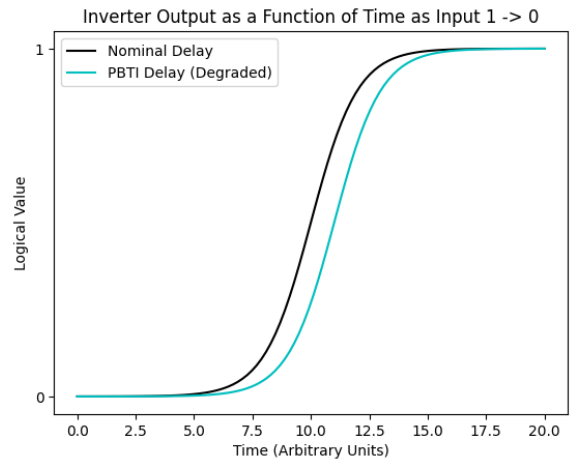
Simple inverter schematic:



Degraded Transistor (PBTI)

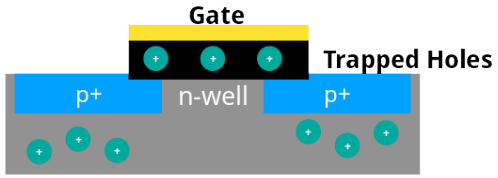


"Positive Bias (+) Temperature Instability"



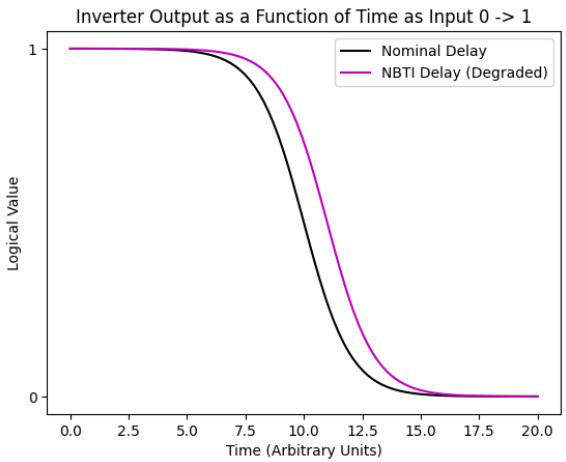
A Pentimenti Emerges

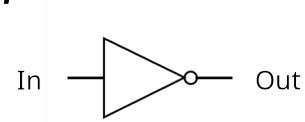
BTI effects create long term measurable timing differences—a pentimenti.

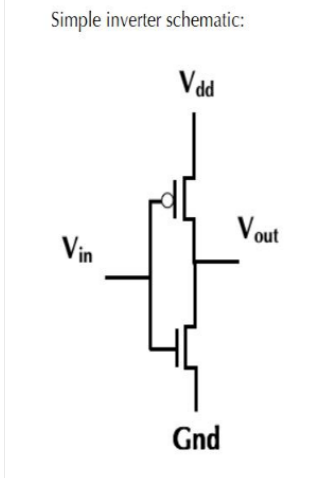


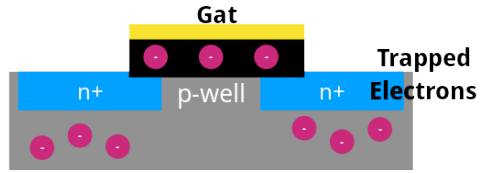
Degraded Transistor (NBTI)

"Negative (-) Bias Temperature Instability"



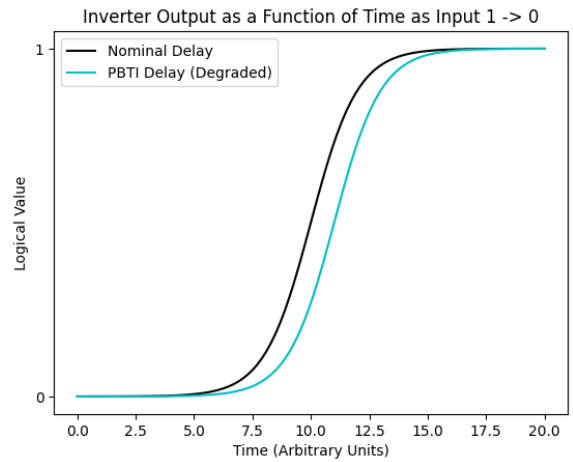






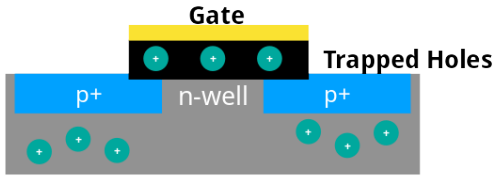
Degraded Transistor (PBTI)

"Positive Bias (+) Temperature Instability"



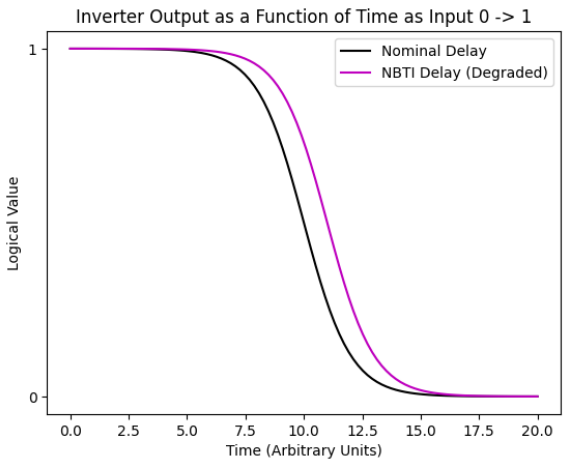
A Pentimenti Emerges

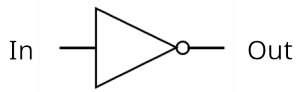
BTI effects create long term measurable timing differences—a pentimenti.

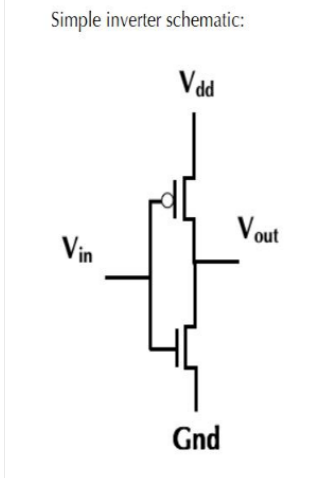


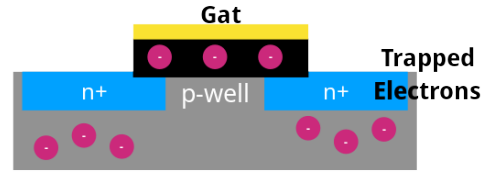
Degraded Transistor (NBTI)

"Negative (-) Bias Temperature Instability"



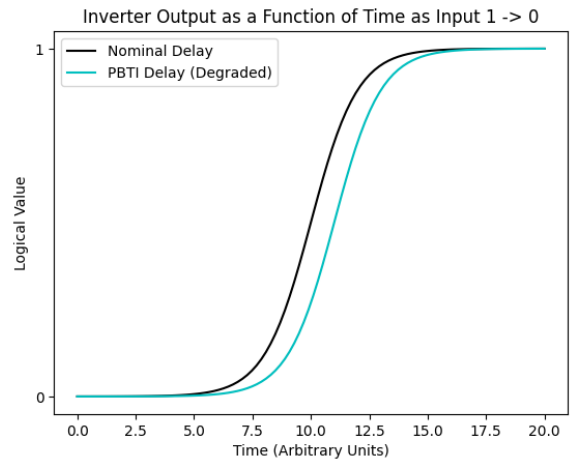






Degraded Transistor (PBTI)

"Positive Bias (+) Temperature Instability"



If we can precisely measure timing through digital components, we can determine the previous logical value they held.

A High-Risk Target

Cloud-Resident FPGAs

A High-Risk Target

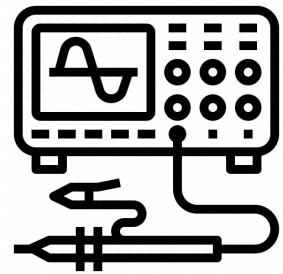
Cloud-Resident FPGAs

- Consecutive users with the expectation of logical isolation.

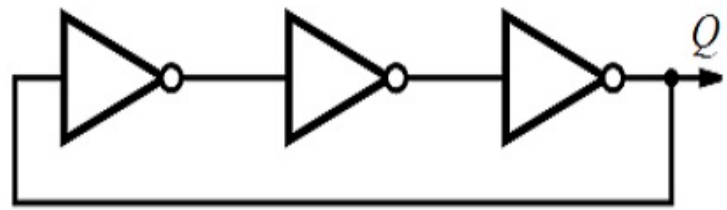
A High-Risk Target

Cloud-Resident FPGAs

- Consecutive users with the expectation of logical isolation.
- BTI has been measured on local FPGAs using conventional means and with PL sensors.



Zick et al. FPL 2014.

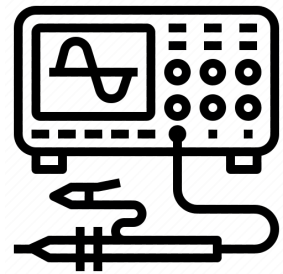


Pfeifer et al. FPL 2013
Amouri et al, FPL 2014
Stott et al. FPGA 2010

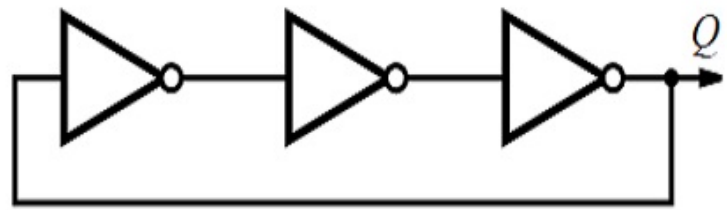
A High-Risk Target

Cloud-Resident FPGAs

- Consecutive users with the expectation of logical isolation.
- BTI has been measured on local FPGAs using conventional means and with PL sensors.
- PL sensors enable a remote attack.



Zick et al. FPL 2014.

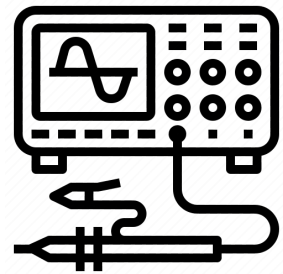


Pfeifer et al. FPL 2013
Amouri et al, FPL 2014
Stott et al. FPGA 2010

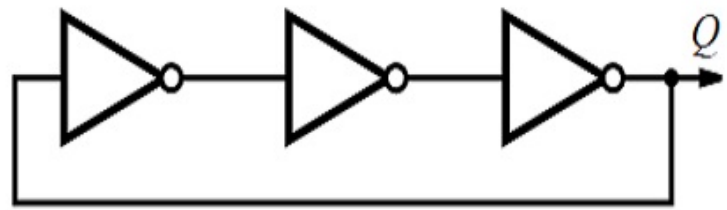
A High-Risk Target

Cloud-Resident FPGAs

- Consecutive users with the expectation of logical isolation.
- BTI has been measured on local FPGAs using conventional means and with PL sensors.
- PL sensors enable a remote attack.
- Never applied to the cloud. Most work focuses on reliability testing, or long term data remanence.

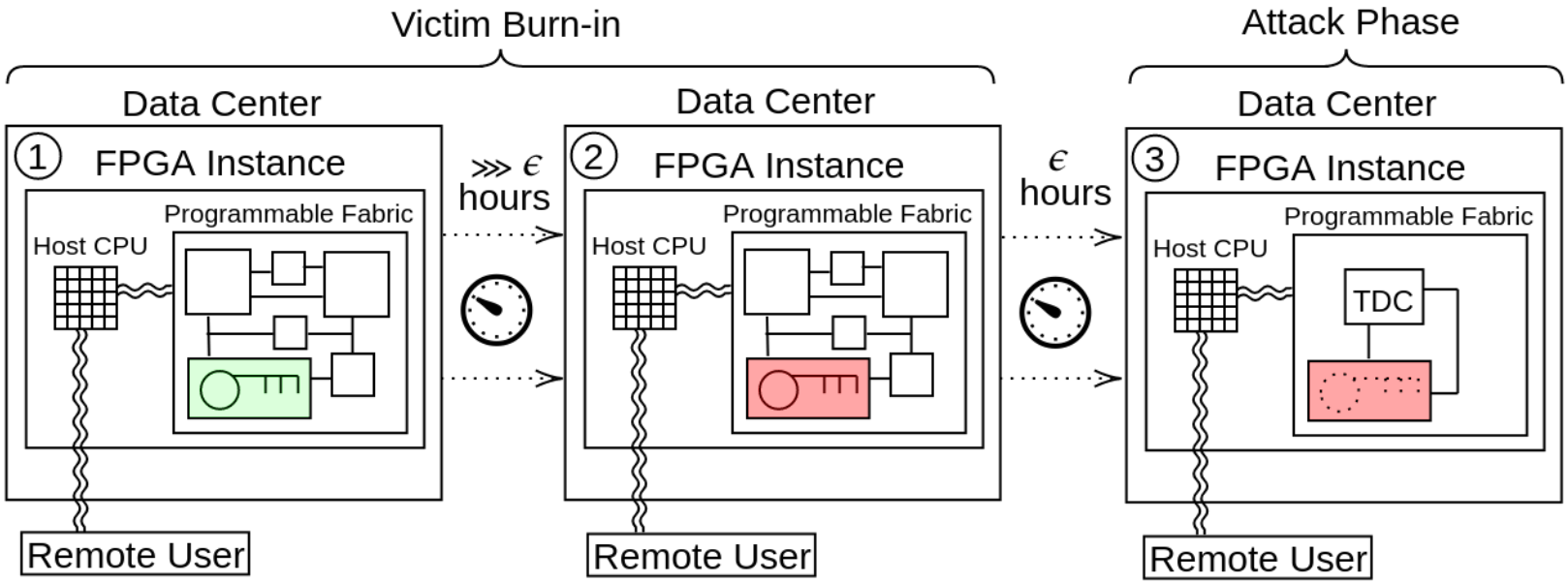


Zick et al. FPL 2014.

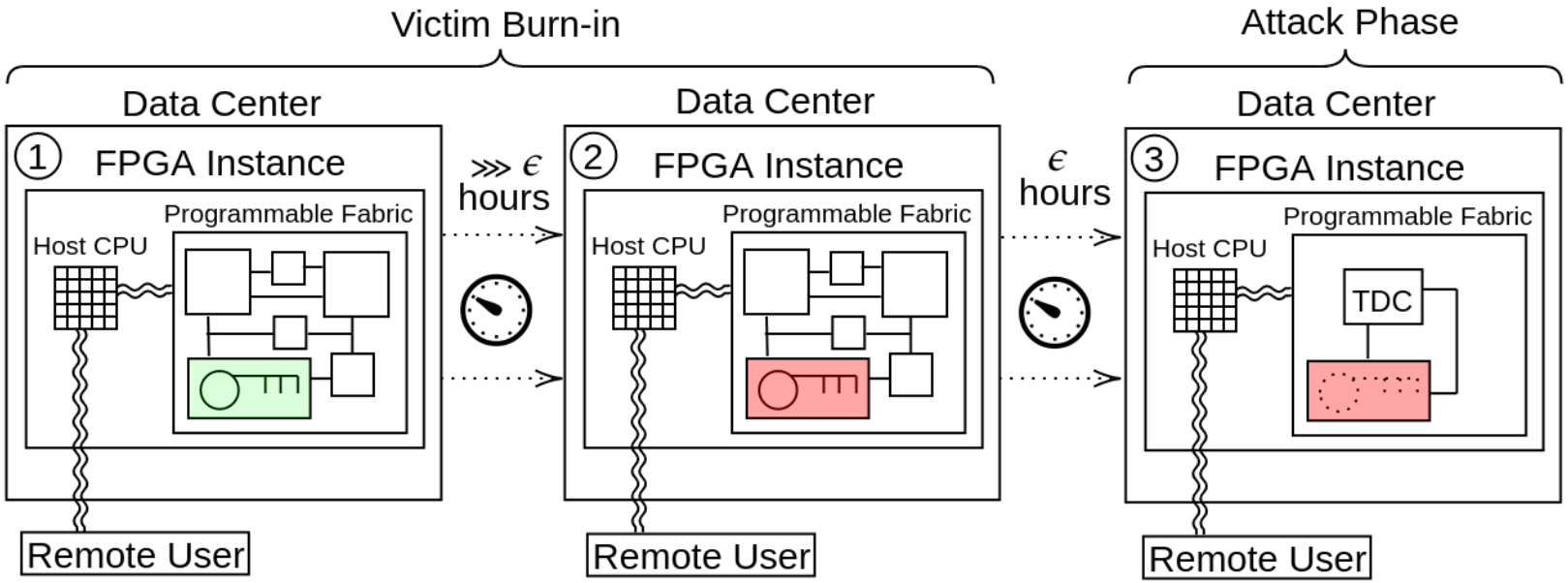


Pfeifer et al. FPL 2013
Amouri et al, FPL 2014
Stott et al. FPGA 2010

Our No-Contact, Legal Circuit, Threat Model

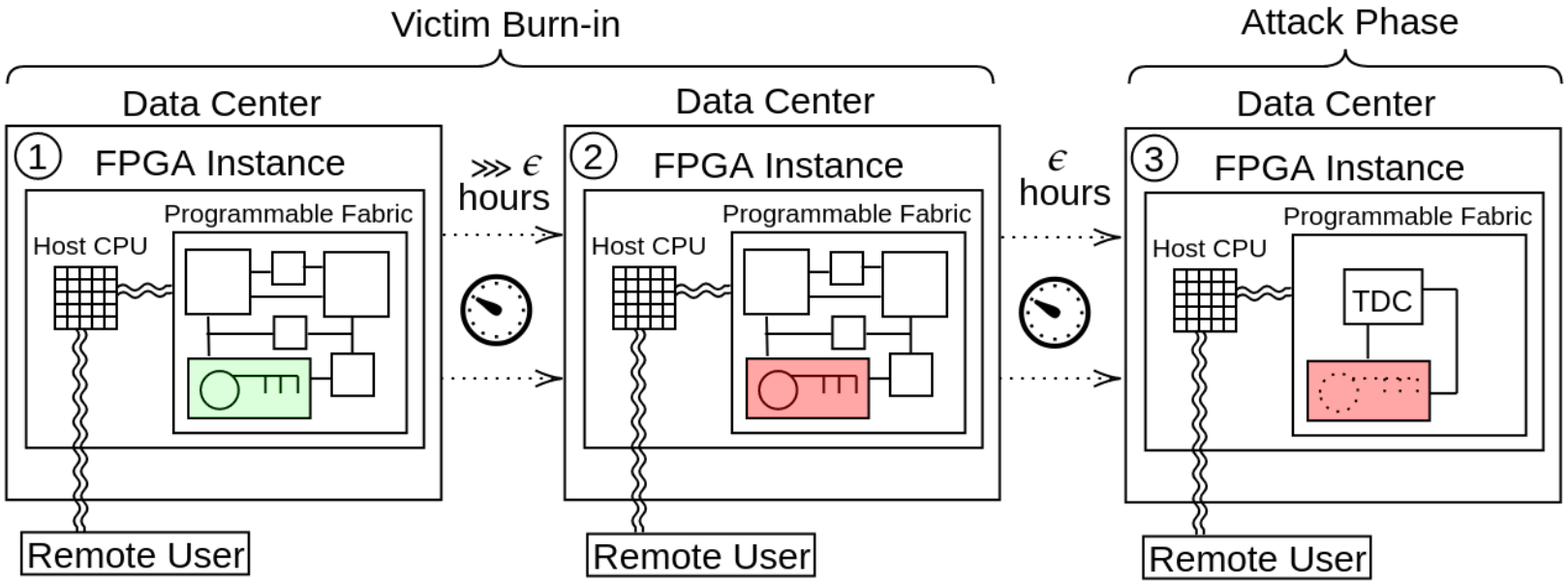


Our No-Contact, Legal Circuit, Threat Model



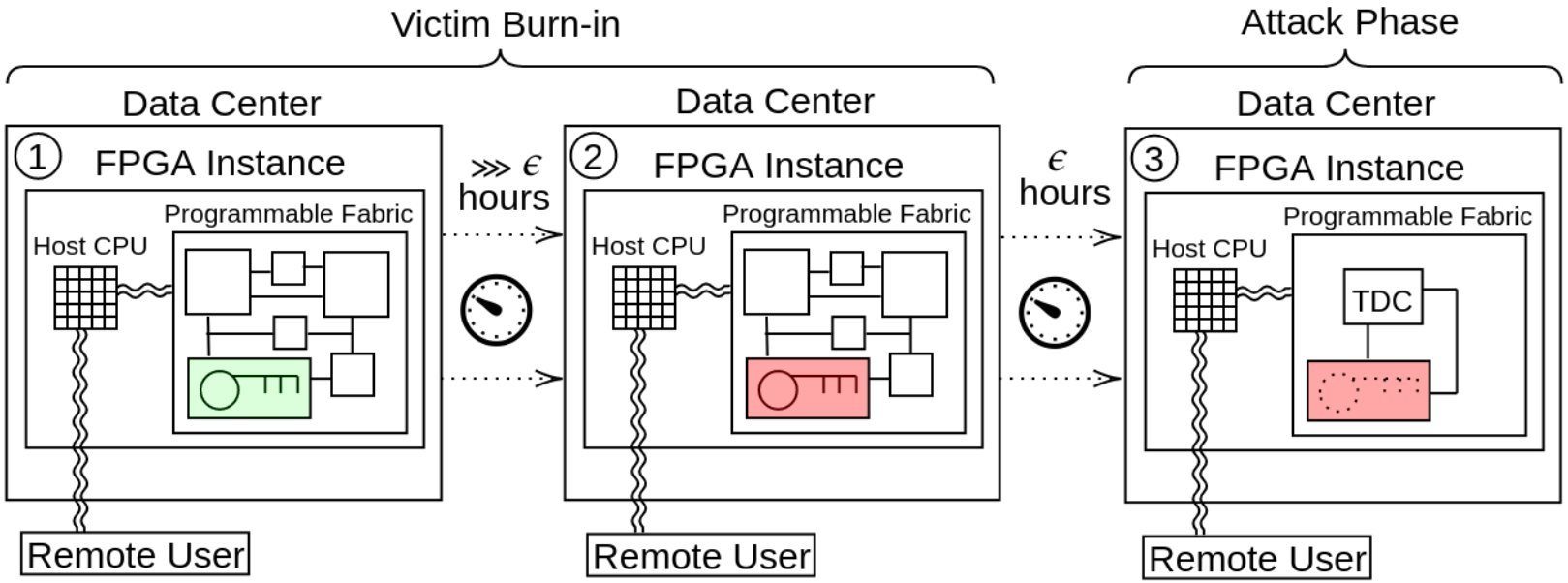
- User rents cloud-FPGA and performs computation using some sensitive data

Our No-Contact, Legal Circuit, Threat Model



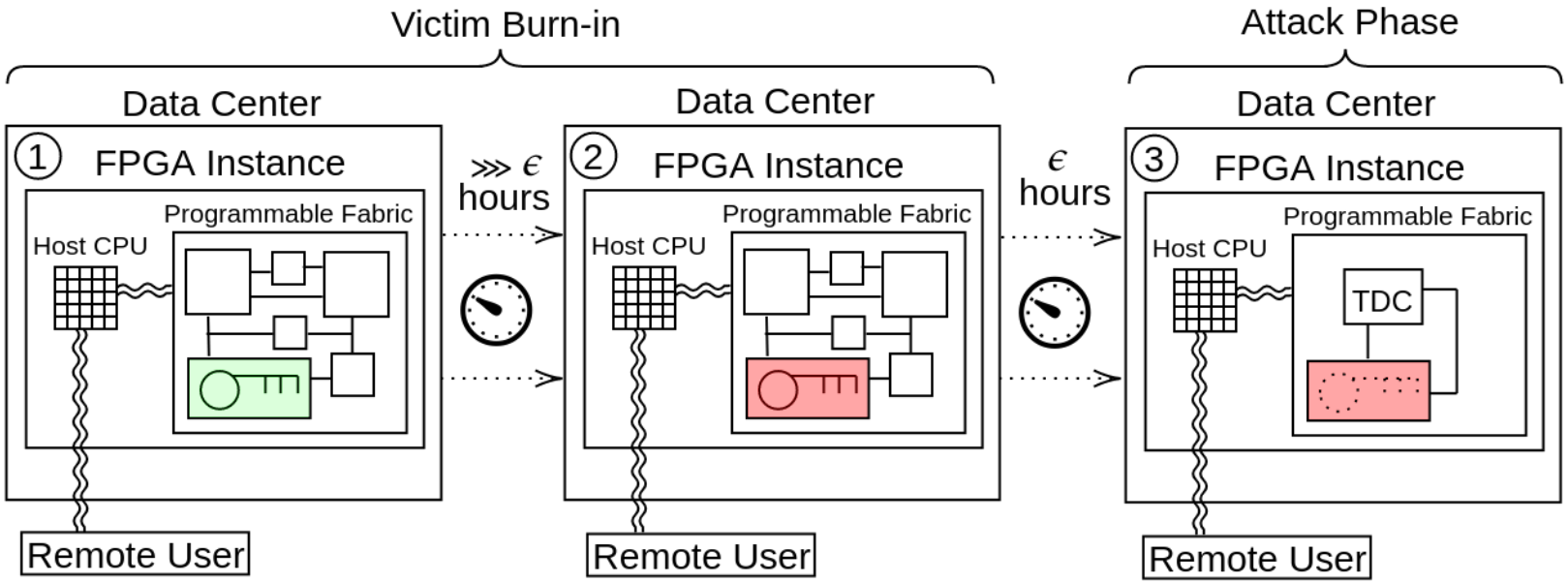
- User rents cloud-FPGA and performs computation using some sensitive data
- Compute....

Our No-Contact, Legal Circuit, Threat Model



- User rents cloud-FPGA and performs computation using some sensitive data
- Compute....
- Relinquish device

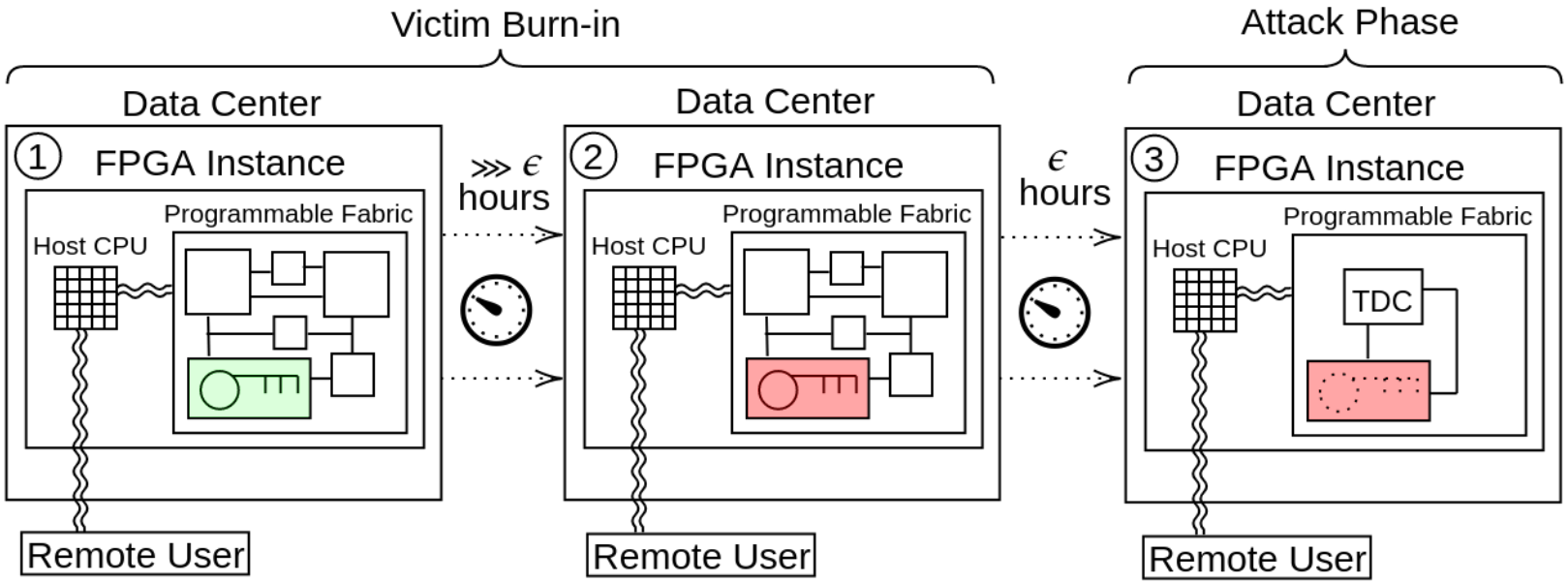
Our No-Contact, Legal Circuit, Threat Model



- User rents cloud-FPGA and performs computation using some sensitive data
- Compute....
- Relinquish device

- Attacker rents boards

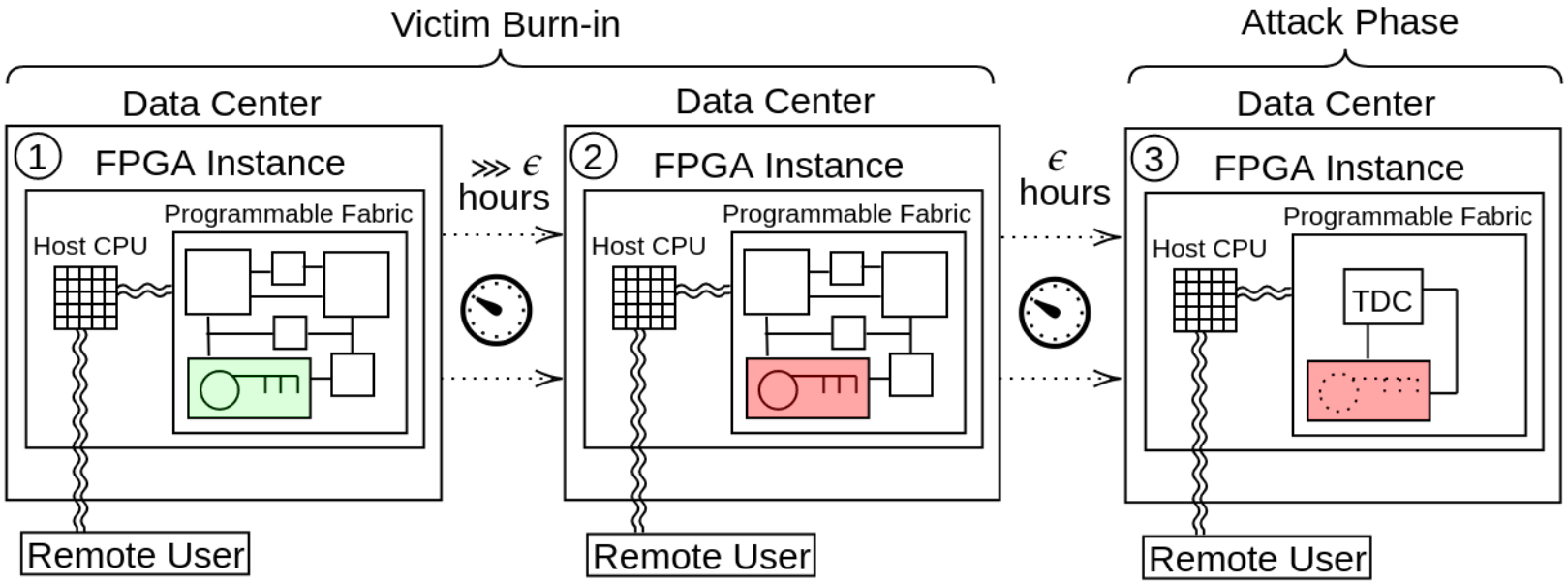
Our No-Contact, Legal Circuit, Threat Model



- User rents cloud-FPGA and performs computation using some sensitive data
- Compute....
- Relinquish device

- Attacker rents boards
- Measures routing which contained sensitive data

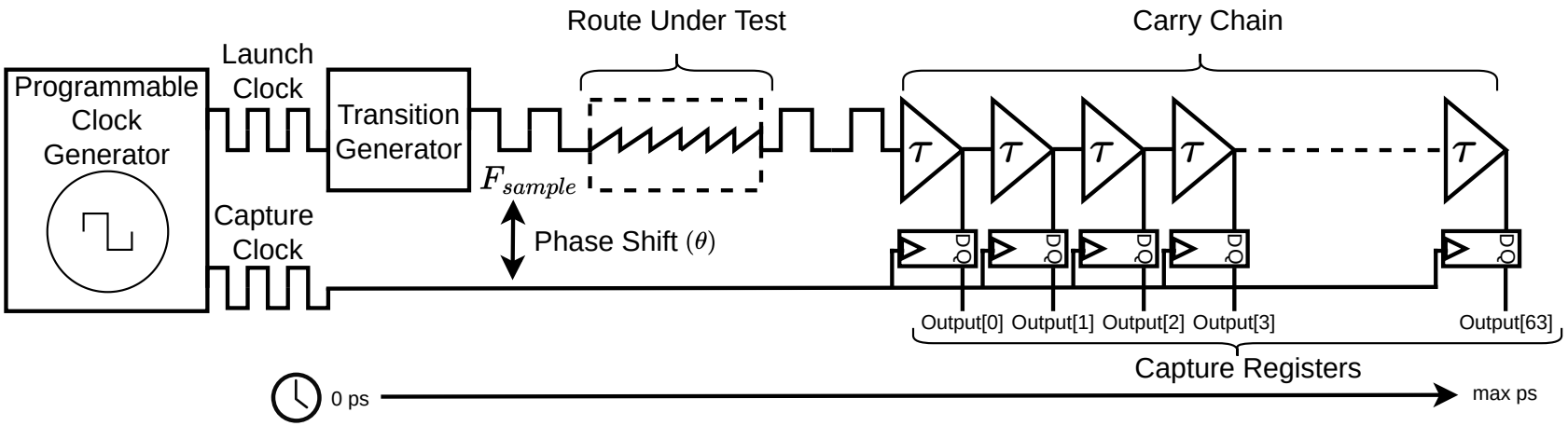
Our No-Contact, Legal Circuit, Threat Model



- User rents cloud-FPGA and performs computation using some sensitive data
- Compute....
- Relinquish device

- Attacker rents boards
- Measures routing which contained sensitive data
- Extract sensitive data

A Totally Legal, No-Contact Sensor



Output Sequence

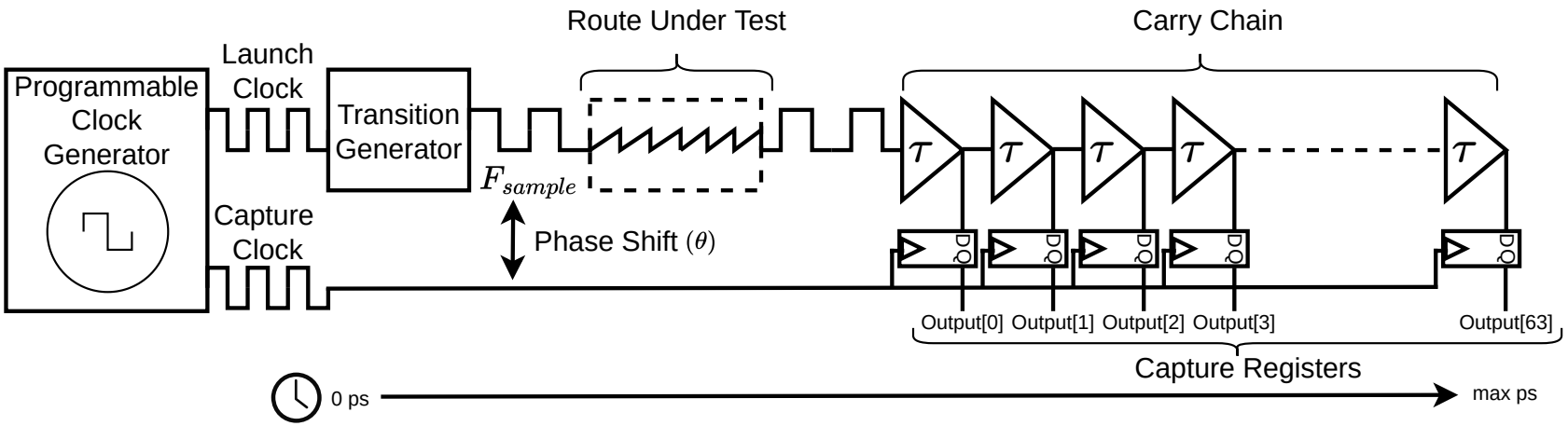
Rising Transition 0: 1111_1111_1111_1111_1111_1111_1111_1111_1111_1110_0000_0000_0000_0000_0000_0000

Falling Transition 0: 0000_0000_0000_0000_0000_0110_1111_1111_1111_1111_1111_1111_1111_1111_1111_1111

Rising Transition 1: 1111_1111_1111_1111_1111_1111_1111_1111_1111_1001_0000_0000_0000_0000_0000_0000

Falling Transition 1: 0000_0000_0000_0000_0000_1010_1111_1111_1111_1111_1111_1111_1111_1111_1111_1111

A Totally Legal, No-Contact Sensor



Output Sequence

Rising Transition 0: 1111_1111_1111_1111_1111_1111_1111_1111_1111_1110_0000_0000_0000_0000_0000_0000

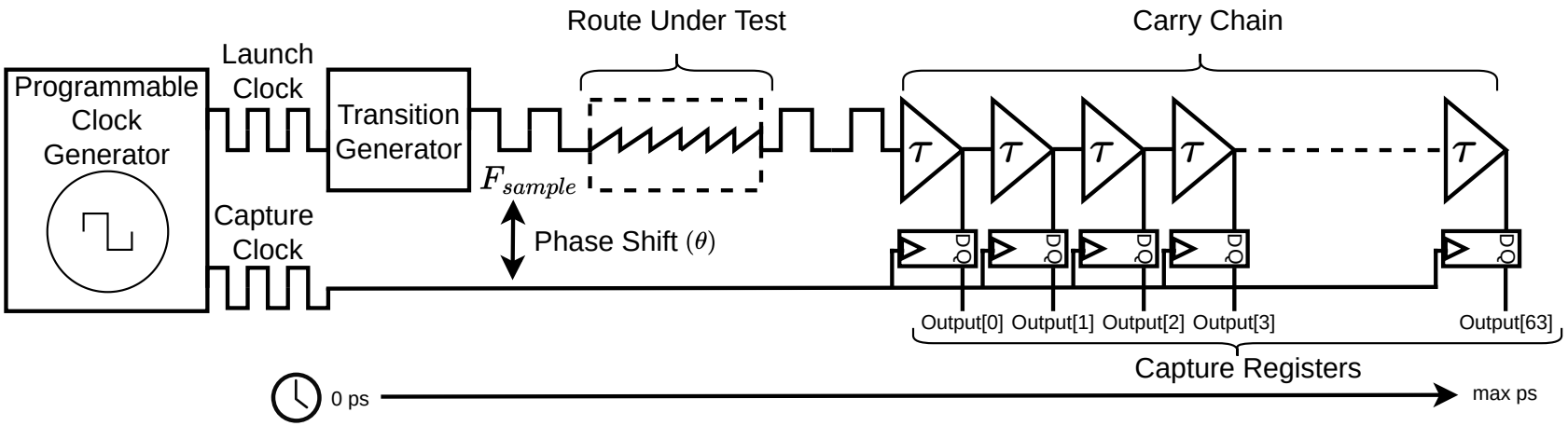
Falling Transition 0: 0000_0000_0000_0000_0000_0110_1111_1111_1111_1111_1111_1111_1111_1111_1111_1111

Rising Transition 1: 1111_1111_1111_1111_1111_1111_1111_1111_1111_1001_0000_0000_0000_0000_0000_0000

Falling Transition 1: 0000_0000_0000_0000_0000_1010_1111_1111_1111_1111_1111_1111_1111_1111_1111_1111

- Undetectable

A Totally Legal, No-Contact Sensor



Output Sequence

Rising Transition 0: 1111_1111_1111_1111_1111_1111_1111_1111_1111_1110_0000_0000_0000_0000_0000_0000

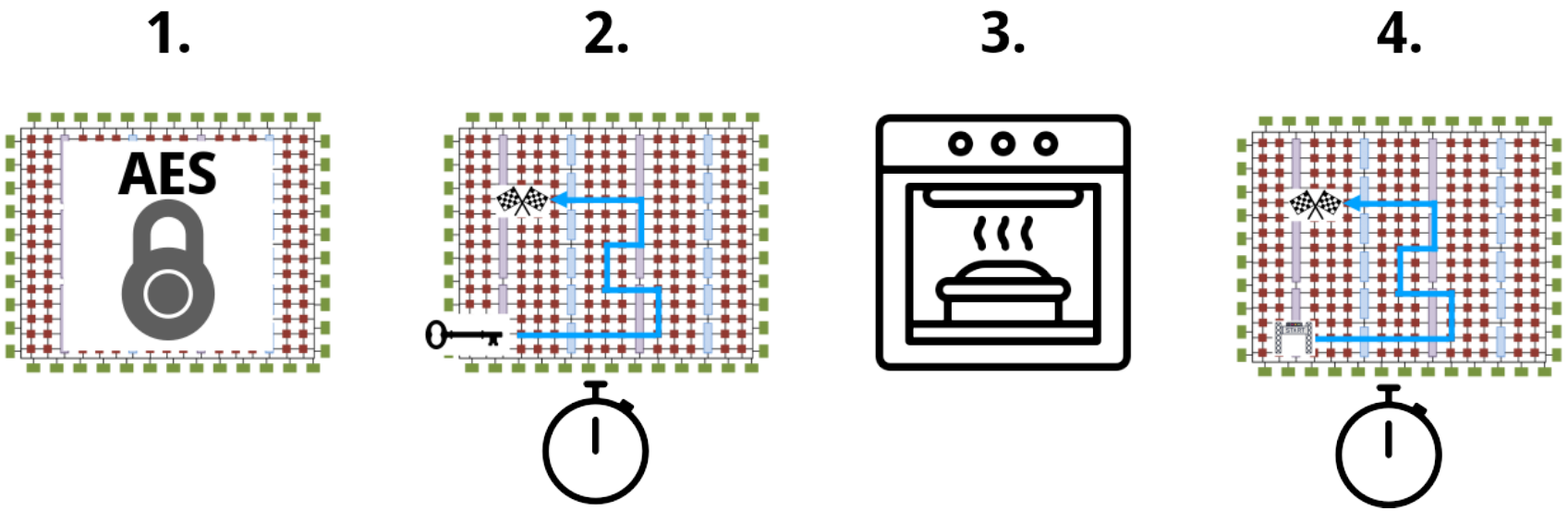
Falling Transition 0: 0000_0000_0000_0000_0000_0110_1111_1111_1111_1111_1111_1111_1111_1111_1111_1111

Rising Transition 1: 1111_1111_1111_1111_1111_1111_1111_1111_1111_1001_0000_0000_0000_0000_0000_0000

Falling Transition 1: 0000_0000_0000_0000_0000_1010_1111_1111_1111_1111_1111_1111_1111_1111_1111_1111

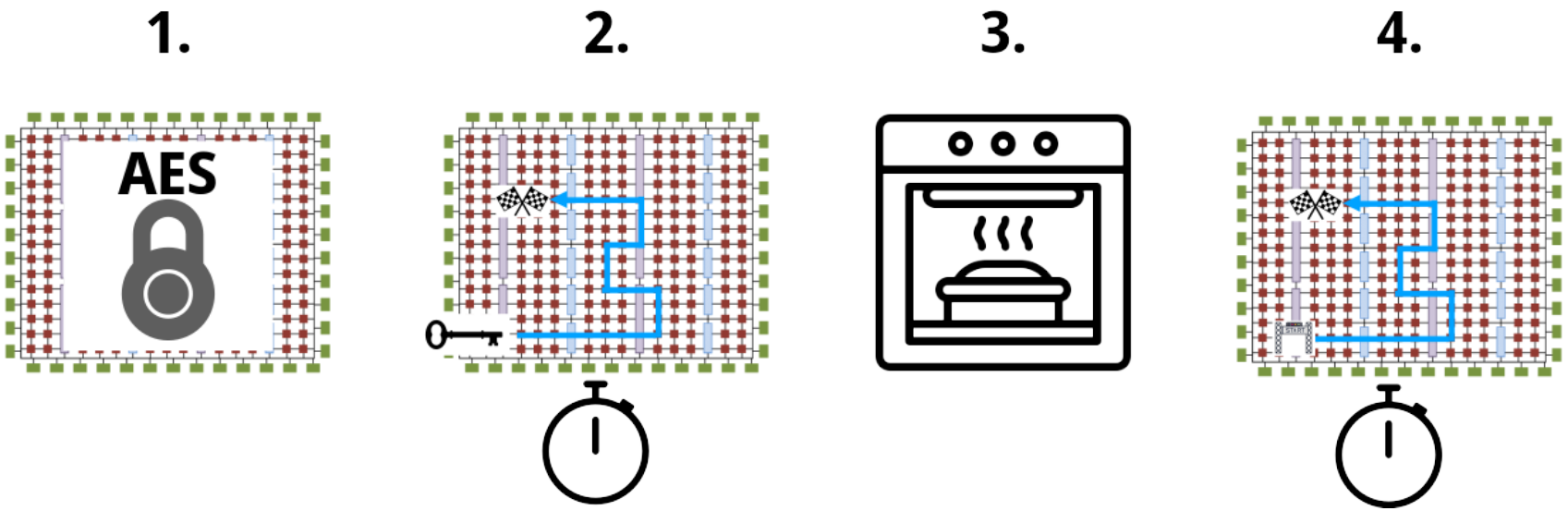
- Undetectable
- Measures timing delay through routing

Experimental Validation



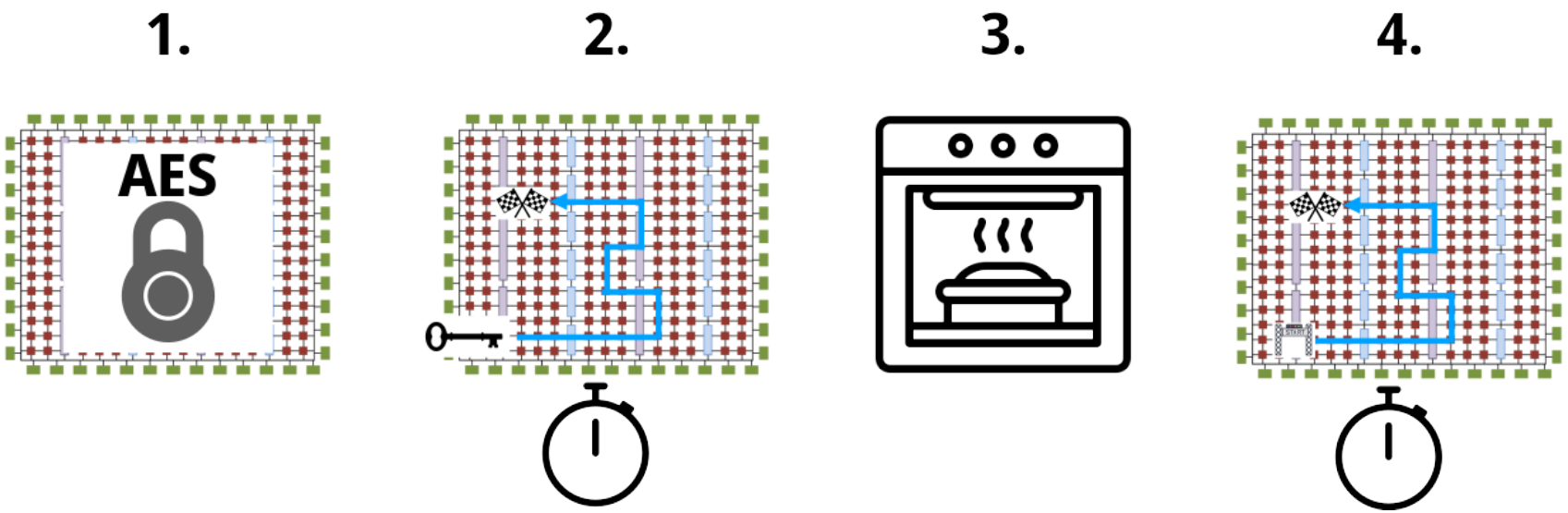
- Instantiate a core that has routes which carry sensitive data

Experimental Validation



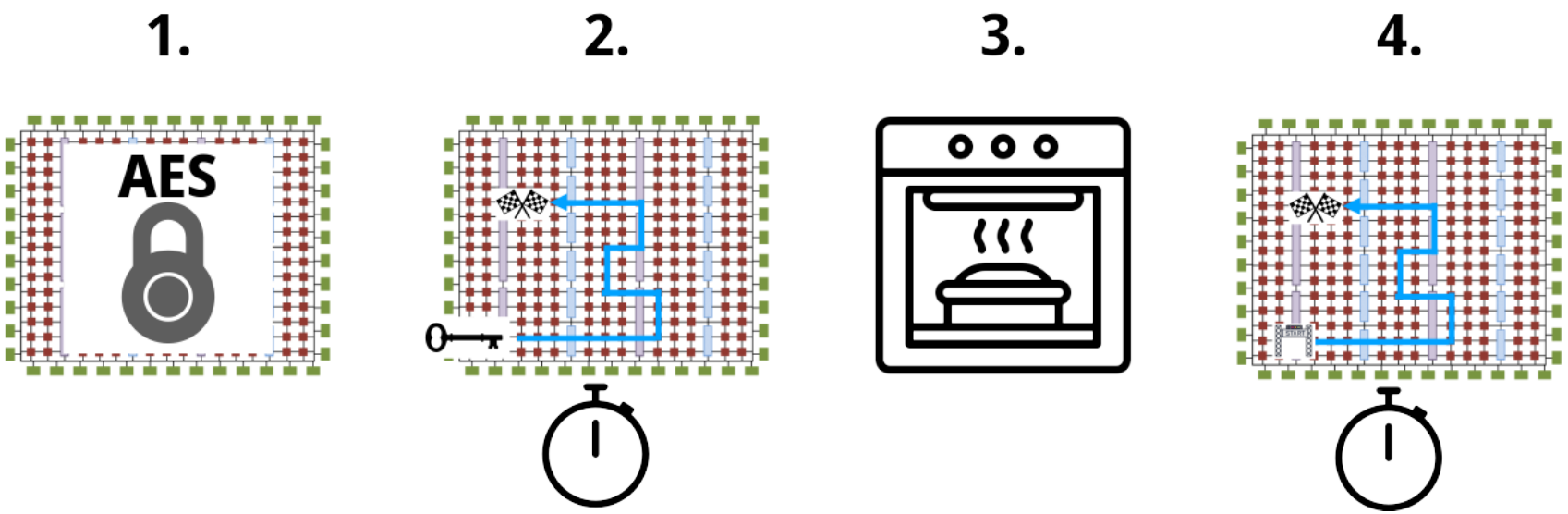
- Instantiate a core that has routes which carry sensitive data
- Bake

Experimental Validation



- Instantiate a core that has routes which carry sensitive data
- Bake
- Load design with TDCs and measure delay

Experimental Validation



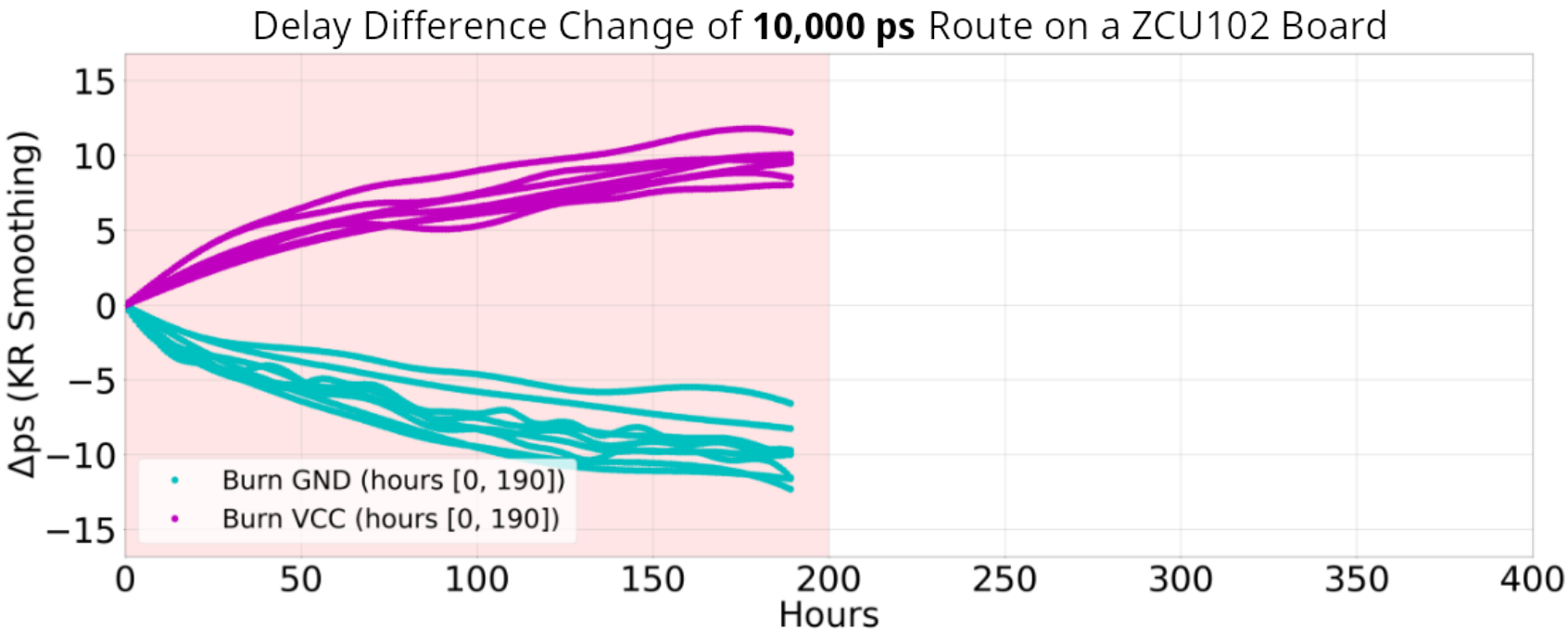
- Instantiate a core that has routes which carry sensitive data
- Bake
- Load design with TDCs and measure delay
- Repeat

Experimental Results — 10000ps Length Routes

Measure delay of sensitive routes as they bake

Experimental Results — 10000ps Length Routes

Measure delay of sensitive routes as they bake

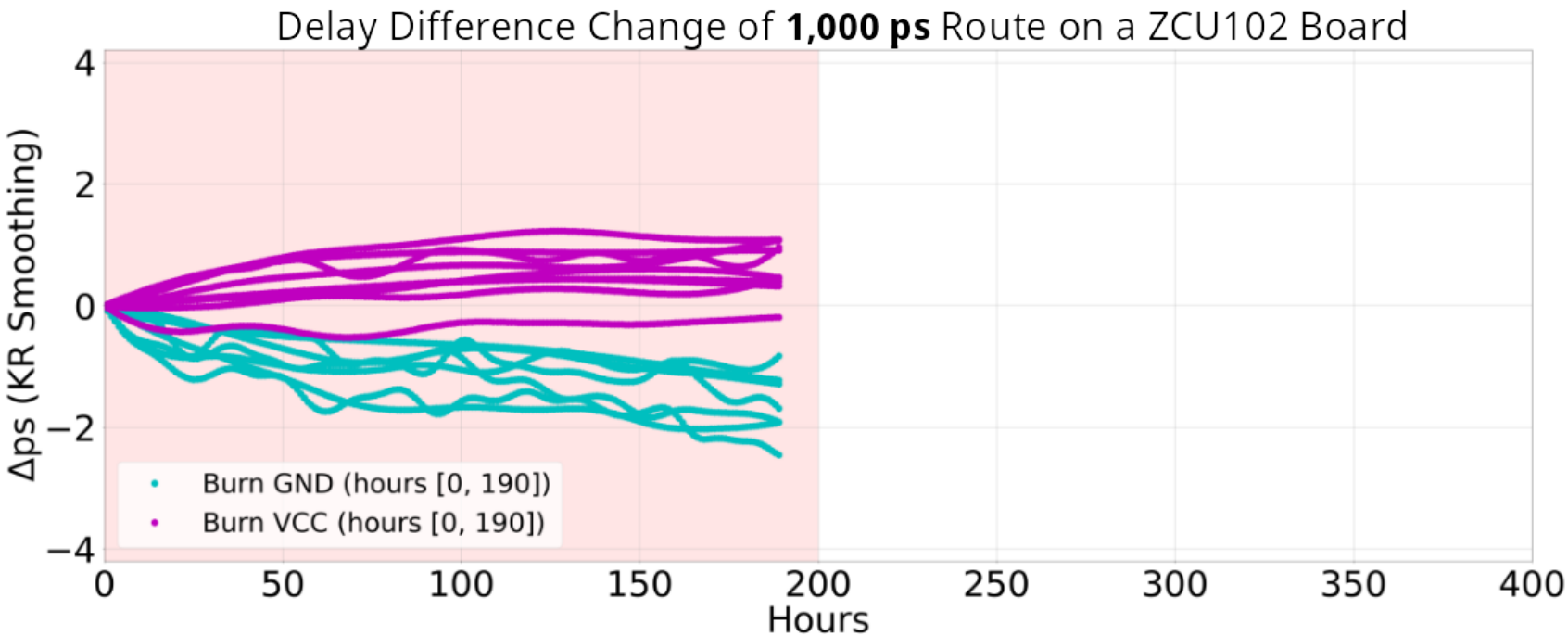


Experimental Results — 1000ps Length Routes

Measure delay of sensitive routes as they bake

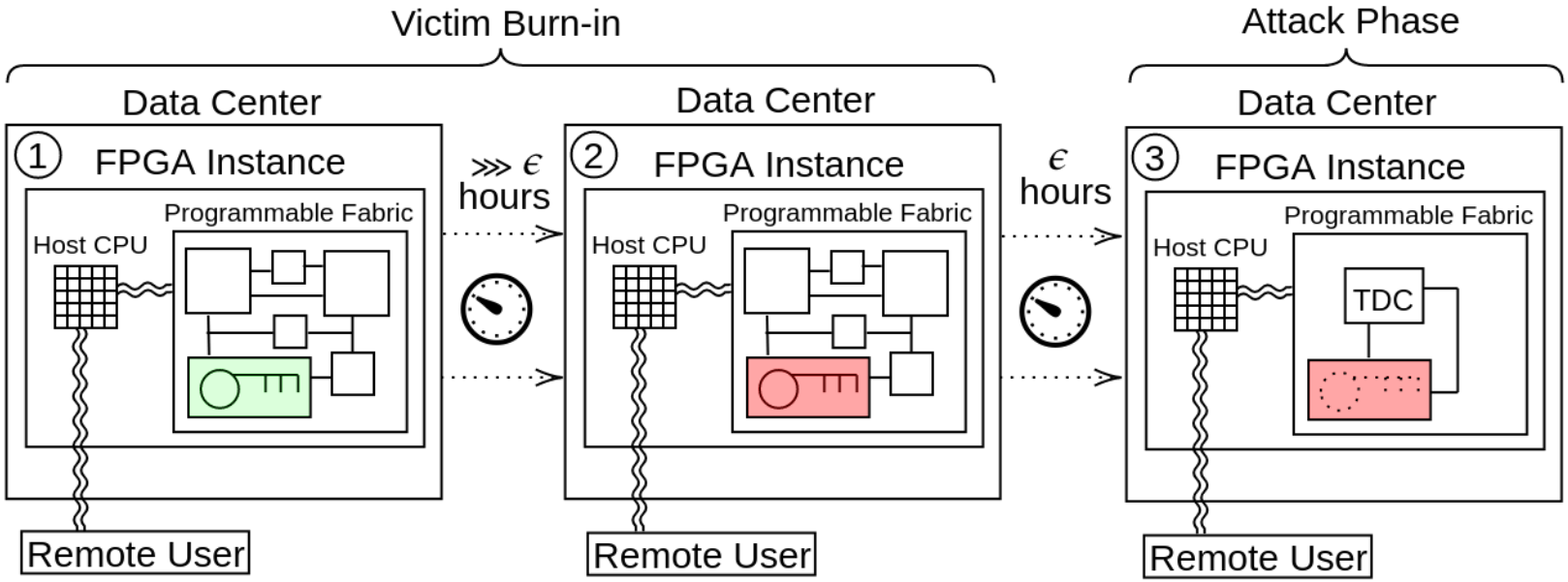
Experimental Results — 1000ps Length Routes

Measure delay of sensitive routes as they bake



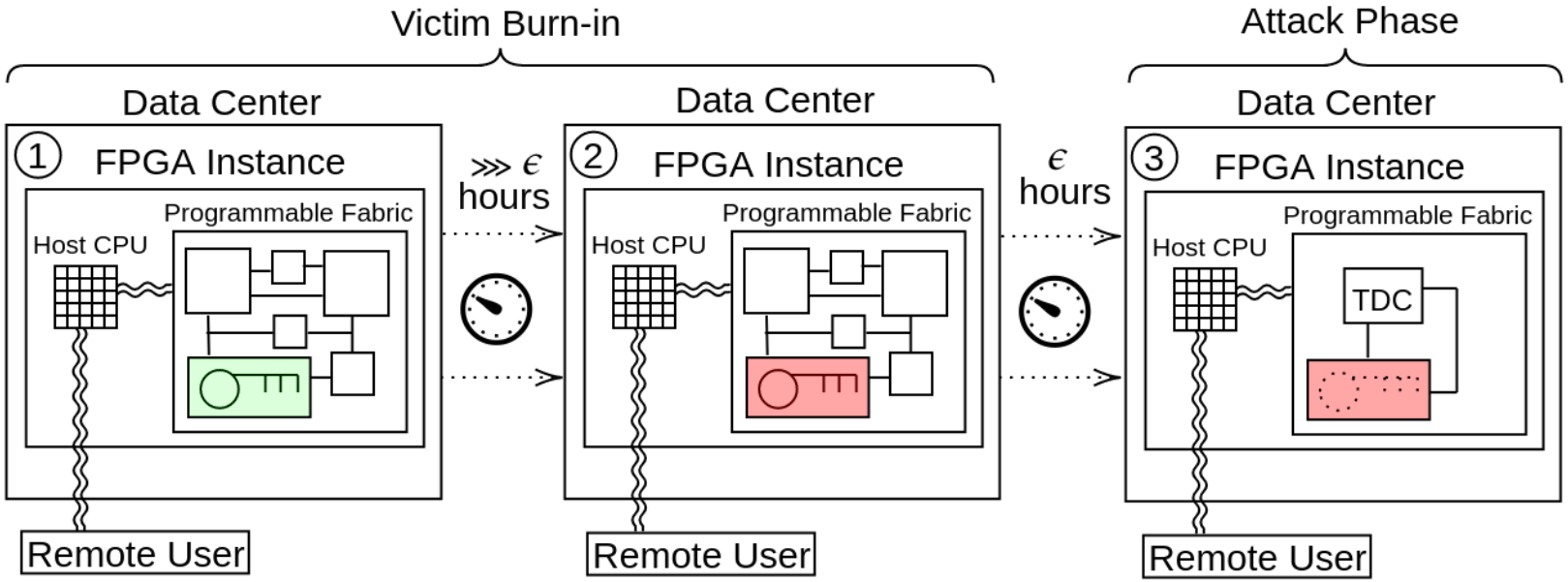
Not Enough For an Attack

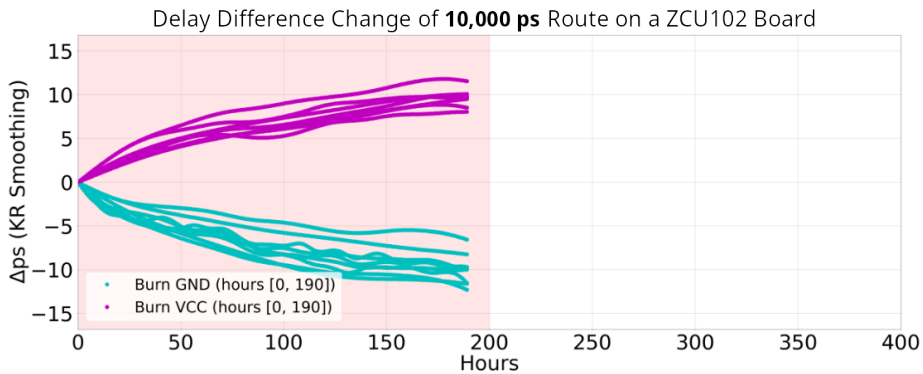
If you recall...



Not Enough For an Attack

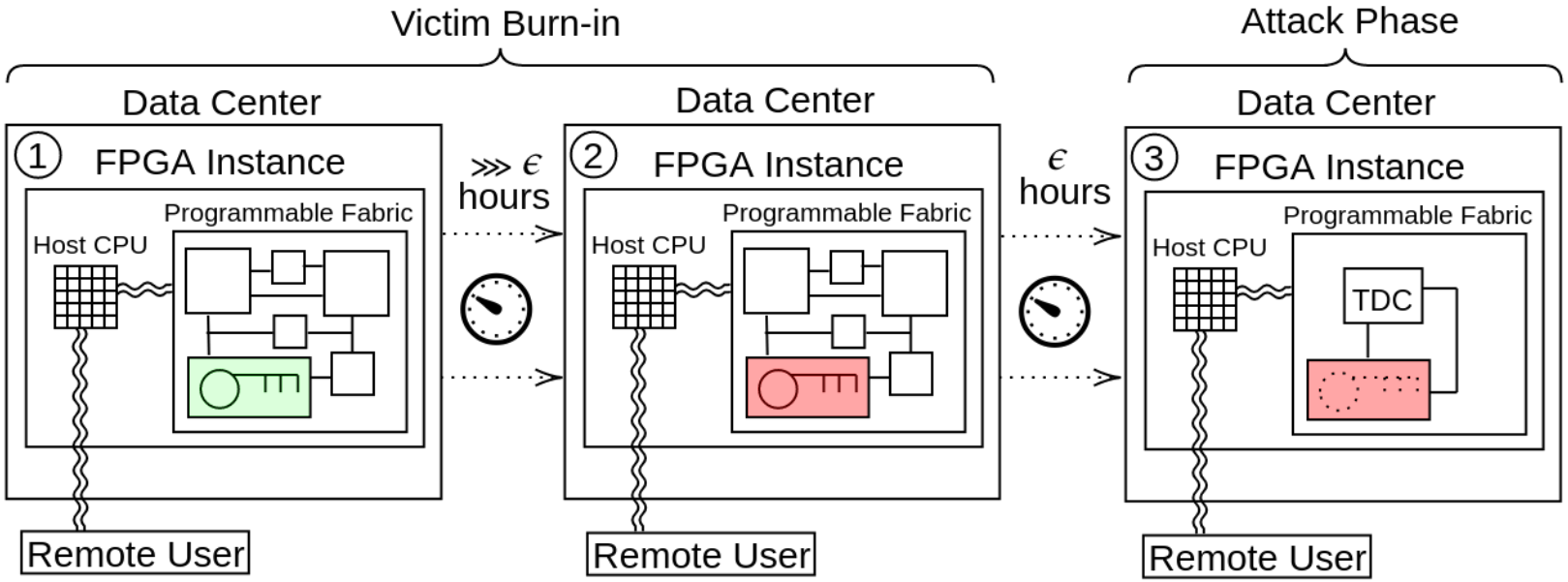
If you recall...

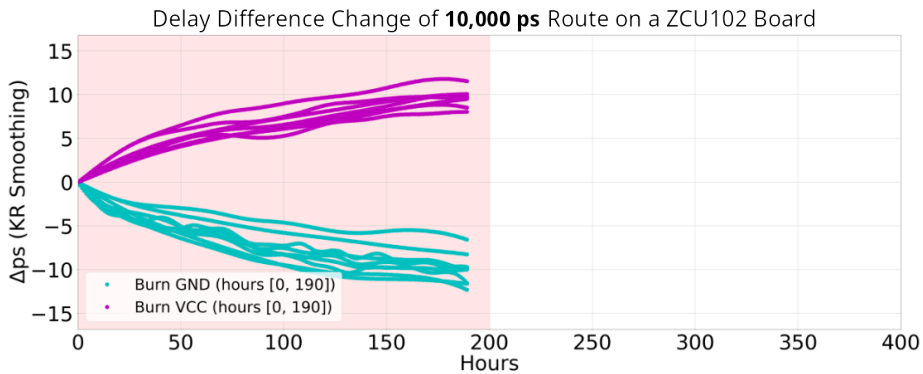




Not Enough For an Attack

If you recall...





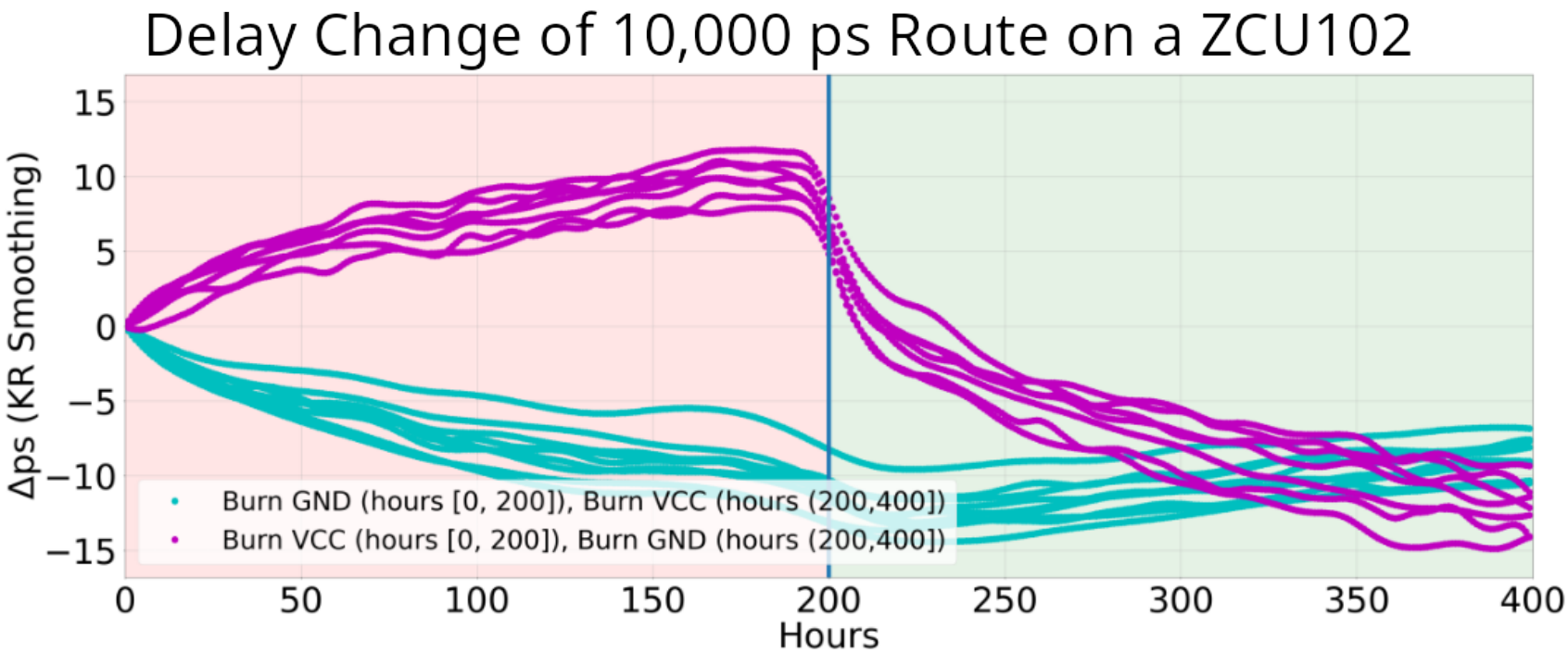
An attacker doesn't know what nominal timing behavior is

An Elastic Effect

Invert the value in sensitive routes

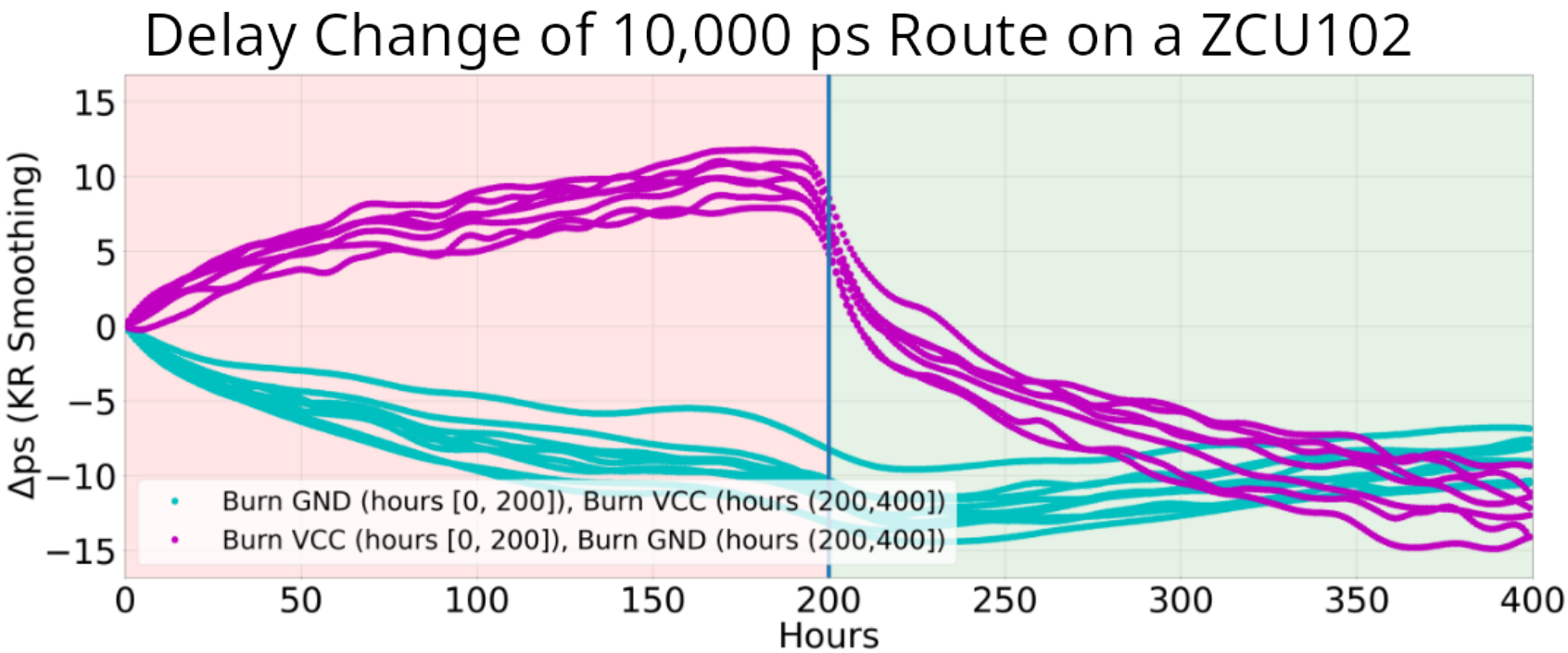
An Elastic Effect

Invert the value in sensitive routes



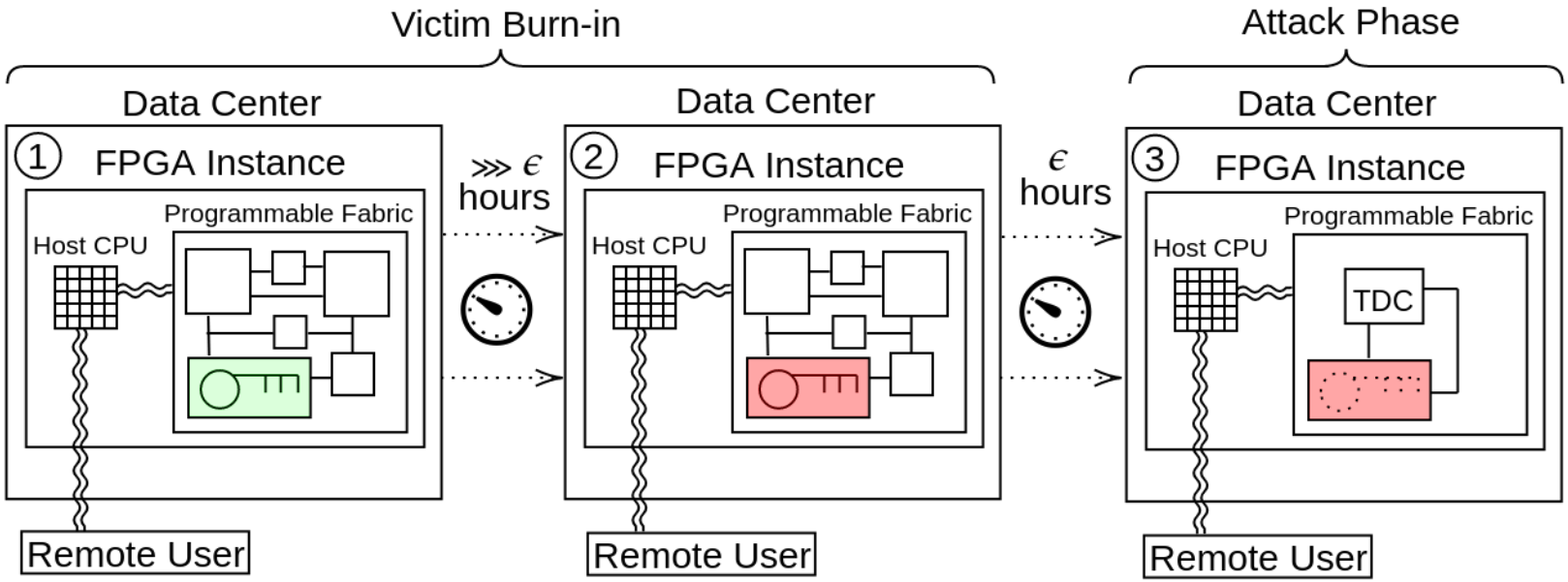
An Elastic Effect

Invert the value in sensitive routes

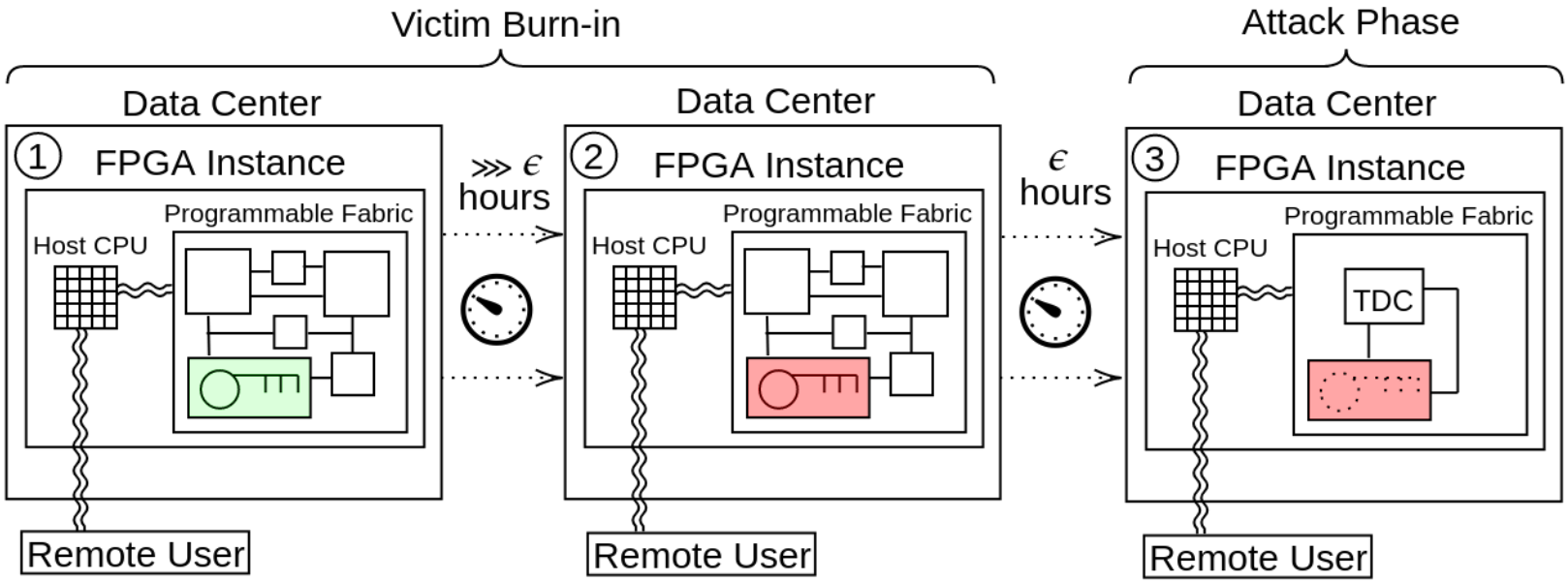


Attacker can apply GND to all routes, study the recovery, and recover original value.

Turning Towards the Cloud...



Turning Towards the Cloud...



Thanks