TU Graz

SCIENCE
PASSION
TECHNOLOGY

Attacking FPGAs with covert channels

Simon Feichter

07.12.2022

Covert Channels in general

What are Covert Channels?

A covert channel is a type of attack that creates a **capability to transfer information objects** between processes that are **not supposed to be allowed to communicate** by the computer security policy.[4]

-Definition by Butler Lampson

What are Covert Channels?

- Hidden communication channel.
- Uses unintended ways of communication.
  - Side Channels
  - Unintended use of protocols.

Side Channels

Leakage of information because of the fundamental way a protocol, algorithm or hardware is implemented.

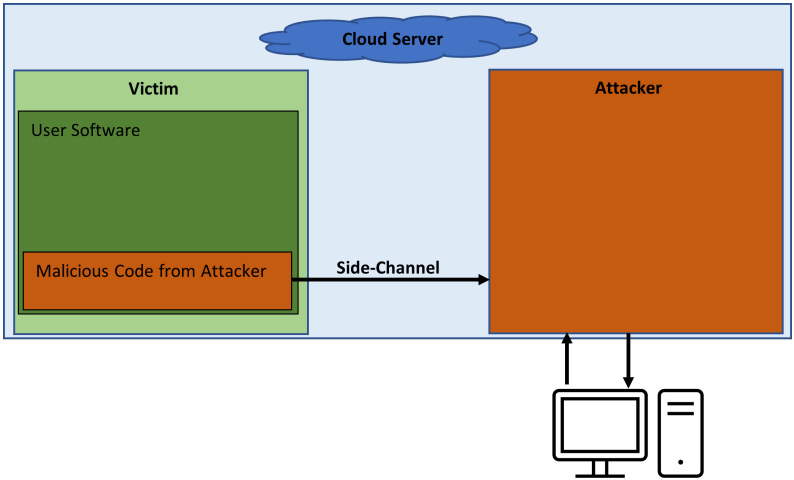
- Timing (Cache Access , execution time .....)
- Voltage level / Power consumption
- Temperature
- .....

Side Channel vs Covert Channel

- Side Channel
  - Extract data from accidental information leakage.
- Covert Channel
  - Deliberately cause side effects and use them as a communication mechanism.

Applications of Covert Channels

- Secretly ex-filtrate data from an infected system.
- Freedom of speech
- Security by obscurity

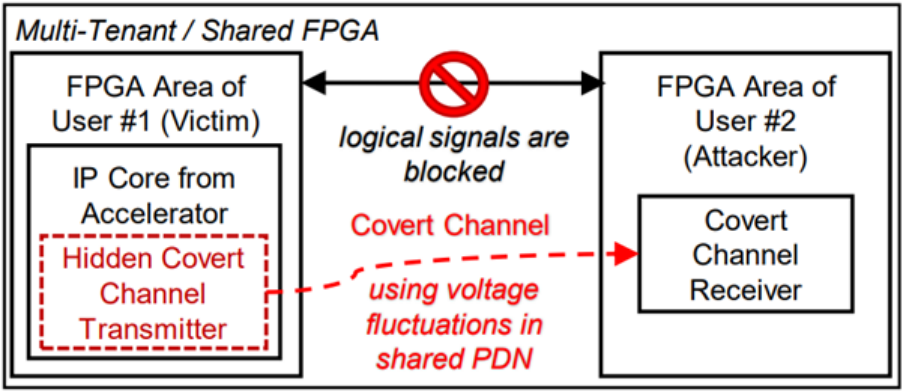

Cloud Server
Victim
User Software
Malicious Code from Attacker
Side-Channel
Attacker

Covert Channels on FPGA's

Multi-Tenant FPGA

- Used in datacenters as hardware accelerators
  - neural networks
  - encryption
  - genome sequencing
- Shared by multiple users

Attacker Model



[2]

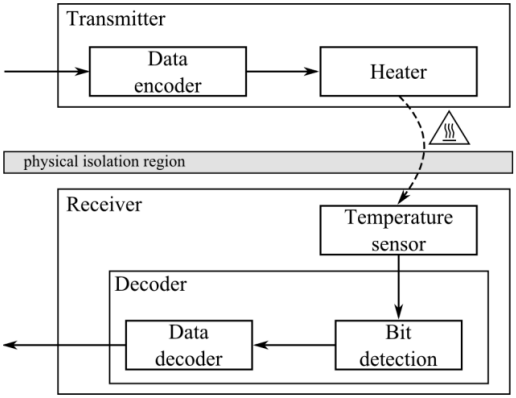
Attacker Model

- The Attacker has partial or complete access to the victim IP core.
- The Attacker has no direct way of communication with the IP core.
- The IP Core fulfills its normal task and has a covert channel to transmit data.
- The FPGA is shared among multiple users, the Attacker has an area on the FPGA where he has full access and therefore can use communication channels.

Possible Side Channels

- Thermal Fluctuations [3]
- Capacitive Coupling / Long Wires [5]
- Voltage Level [2] [1]

Thermal Fluctuations

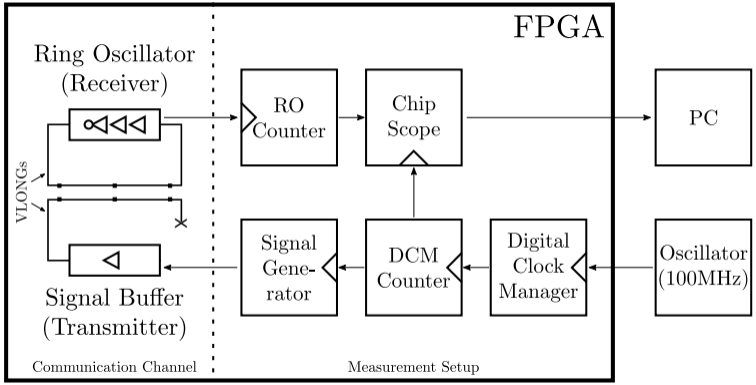


[3]

Thermal Fluctuations

- RO or overclocked shift register as heater
- RO with Counter as sensor
- Limited speed, because heating/cooling is a slow process
- 1 Bit/s

Long Wires


FPGA
Ring Oscillator
(Receiver)
VLONGs
Signal Buffer
(Transmitter)
RO
Counter
Chip
Scope
PC
Signal
Gene-
rator
DCM
Counter
Digital
Clock
Manager
Oscillator
(100MHz)
Communication Channel
Measurement Setup

[5]

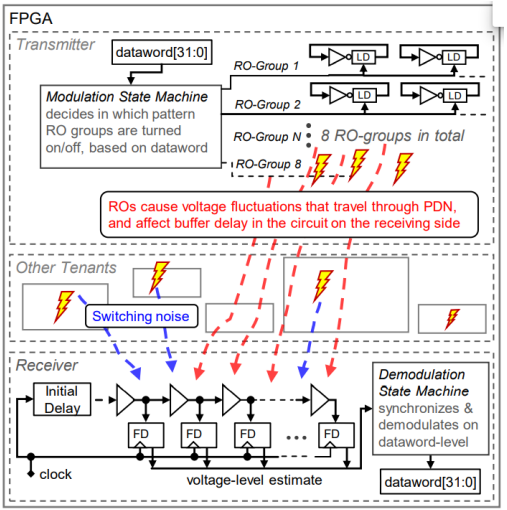
Long Wires

- State of "long-wires" influence the delay of nearby wires.
- Requres a specific Layout and a close proximity between Victim and Attacker
- 6kbps
- Prevented by guard slices between IP cores

Voltage-based Covert Channels

Voltage-based Covert Channels

- Use the Power Distribution Network as shared bus.
- Use Ring Oscillators as transmitter
- Use Time-to-Digital-Converters as receiver


FPGA
Transmitter
dataword[31:0]
Modulation State Machine
decides in which pattern
RO groups are turned
on/off, based on dataword
RO-Group 1
RO-Group 2
RO-Group N
RO-Group 8
8 RO-groups in total
LD
ROs cause voltage fluctuations that travel through PDN,
and affect buffer delay in the circuit on the receiving side
Other Tenants
Switching noise
Receiver
Initial
Delay
FD
clock
voltage-level estimate
Demodulation
State Machine
synchronizes &
demodulates on
dataword-level
dataword[31:0]

[2]

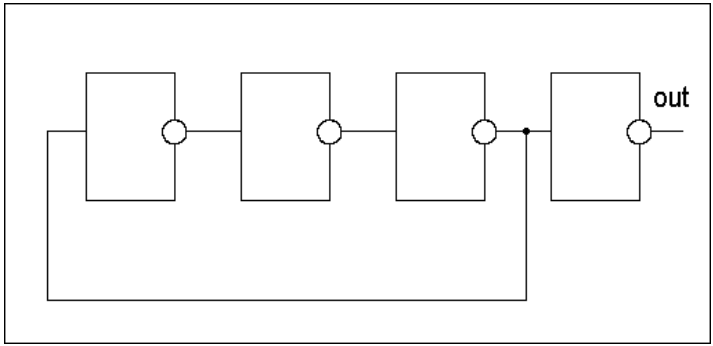
Power Distribution Network (PDN)

Shared for all IP Cores on the Multi-Tenant FPGA, provides power and tries to keep the voltage constant.

- $P \propto f \cdot V^2$
- $\tau_d \propto \frac{1}{V}$

Due to parasitic resistive and inductive components, switching influences the Voltage level.

Ring Oscillator (RO)



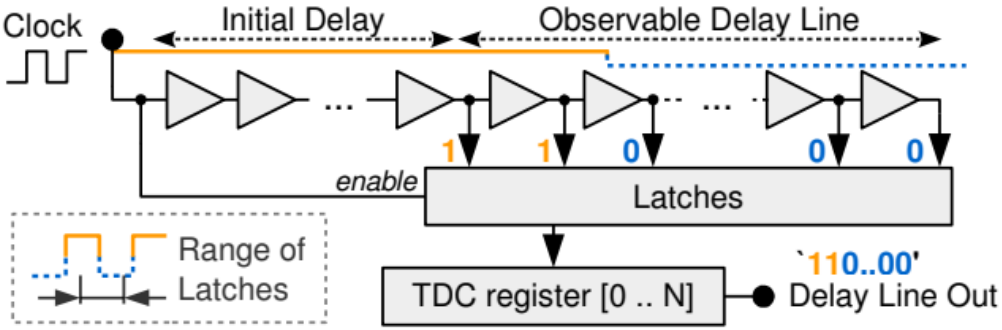
Ring Oscillator (RO)

- Fast switching, frequency is only limited by propagation delay.
- Enable-Signal to start/stop the ROs.
- Suddenly activating multiple ROs leads to a voltage drop.
- Output frequency can be used to measure the voltage.

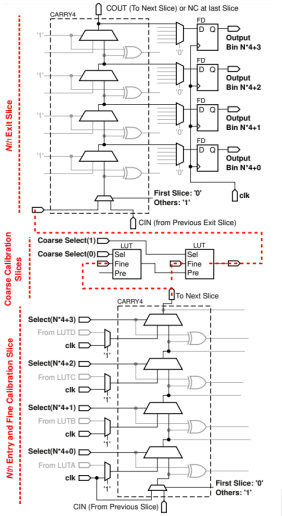
Time-to-Digital-Converters (TDC)

- Rely on the difference in circuit speed, depending on the voltage level
- Uses a cascade of buffers as a single long path
- Registers show how far the signal propagates within one clock cycle and thus give information about the voltage level.

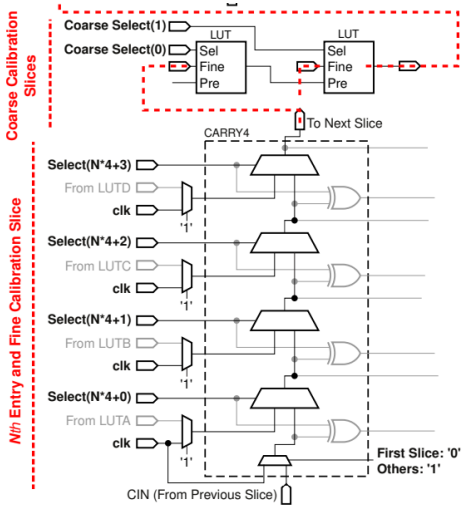
Time-to-Digital-Converters (TDC)

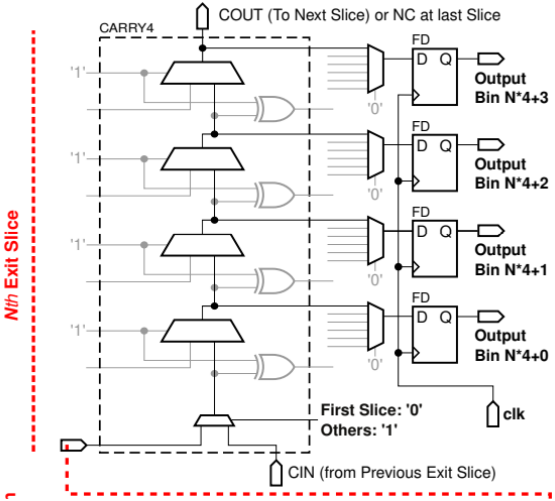


[1]

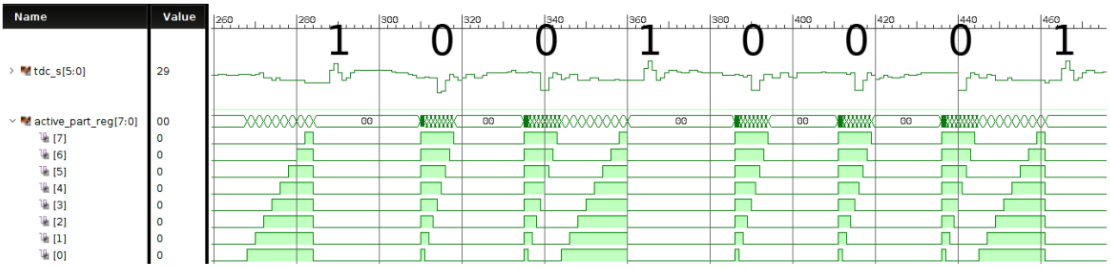

COUT (To Next Slice) or NC at last Slice
CARRY4
FD
Output Bin N*4+3
Output Bin N*4+2
Output Bin N*4+1
Output Bin N*4+0
First Slice: '0'
Others: '1'
clk
CIN (from Previous Exit Slice)
N/4 Exit Slice
Coarse Select(1)
Coarse Select(0)
LUT
Sel
Fine
Pre
Coarse Calibration Slices
To Next Slice
Select(N*4+3)
Select(N*4+2)
Select(N*4+1)
Select(N*4+0)
From LUTD
From LUTC
From LUTB
From LUTA
N/4 Entry and Fine Calibration Slice
CIN (From Previous Slice)

[2]


Coarse Calibration Slices
Coarse Select(1)
Coarse Select(0)
LUT
Sel
Fine
Pre
LUT
Sel
Fine
Pre
To Next Slice
CARRY4
Nth Entry and Fine Calibration Slice
Select(N*4+3)
From LUTD
clk
'1'
Select(N*4+2)
From LUTC
clk
'1'
Select(N*4+1)
From LUTB
clk
'1'
Select(N*4+0)
From LUTA
clk
'1'
First Slice: '0'
Others: '1'
CIN (From Previous Slice)


COUT (To Next Slice) or NC at last Slice
CARRY4
FD
D Q
Output
Bin N*4+3
Output
Bin N*4+2
Output
Bin N*4+1
Output
Bin N*4+0
'1'
'0'
Nth Exit Slice
First Slice: '0'
Others: '1'
clk
CIN (from Previous Exit Slice)

Transmission



[2]

Transmission

3 possible states:

- Negative spike $\rightarrow$ 0
  - Enable all ROs at once, disable slowly
- Positive spike $\rightarrow$ 1
  - Enable ROs slowly, disable all at once
- No spike

Receiver

Noise because of multiple IP-Cores on the FPGA, a detection algorithm is required.

- Threshold-based strategy
  - Statically defined threshold after expirements.
  - Problem : The TDC result drifts over time because of temperature-dependency
- Gradient-Estimation-based strategy

Receiver

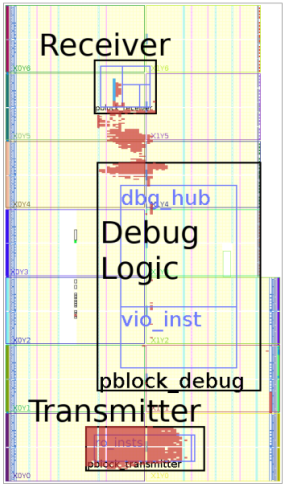
Noise because of multiple IP-Cores on the FPGA, a detection algorithm is required.

- Threshold-based strategy
- Gradient-Estimation-based strategy
  - Buffer TDC Value and calculate gradient between them.
  - Problem: The raise / fall of the voltage level can take more than on cycle

Implementation by Dennis R. E. Gnad , Cong Dang Khoa Nguyen , Syed Hashim Gillani and Mehdi B. Tahoori

- Xilinx Pynq-Z1 board
- Xilinx FPGA SOC
- Dual-Core ARM Cortex-A9 CPU

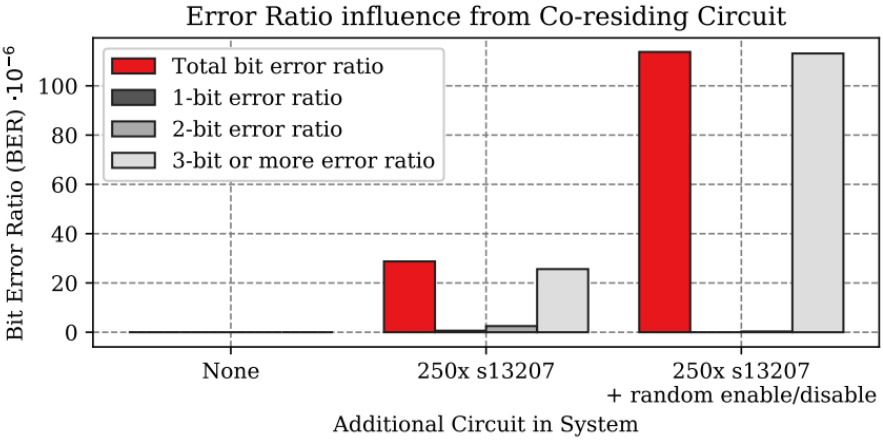
- Receiver (200MHz)
  - 1.02% of all Slices
  - 0.73% of all LUTs
  - 0.35% of all Registers
- Transmitter
  - 5.45% of all Slices
  - 5% of all LUTs
  - 2.5% of all Registers



[2]

Results

- Up to 8Mbit/s Transmission rate
- 0.003% Error-Rate (Depending on System Utilization)


Error Ratio influence from Co-residing Circuit
Total bit error ratio
1-bit error ratio
2-bit error ratio
3-bit or more error ratio
Bit Error Ratio (BER) ·10⁻⁶
0
20
40
60
80
100
None
250x s13207
250x s13207
+ random enable/disable
Additional Circuit in System

[2]

[1] Dennis R.E. Gnad et al. **Analysis of transient voltage fluctuations in FPGAs**. 2016 International Conference on Field-Programmable Technology (FPT). 2016, pp. 12–19. DOI: 10.1109/FPT.2016.7929182.

[2] Dennis RE Gnad et al. **Voltage-Based Covert Channels Using FPGAs**. *ACM Transactions on Design Automation of Electronic Systems (TODAES)* 26.6 (2021), pp. 1–25.

[3] Taras Iakymchuk, Maciej Nikodem, and Krzysztof Kępa. **Temperature-based covert channel in FPGA systems**. 6th International Workshop on Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC). IEEE. 2011, pp. 1–7.

[4] Butler W. Lampson. **A Note on the Confinement Problem**. *Commun. ACM* 16.10 (Oct. 1973), pp. 613–615. ISSN: 0001-0782. DOI: 10.1145/362375.362389. URL: https://doi.org/10.1145/362375.362389.

[5] George Provelengios et al. **Characterization of long wire data leakage in deep submicron FPGAs**. Proceedings of the 2019 ACM/SIGDA International