Measuring Long Wire Leakage with Ring Oscillators in Cloud FPGAs

Ilias Giechaskiel[†‡] Kasper B. Rasmussen[†] Jakub Szefer [‡]

9 September 2019

[†] University of Oxford

[‡] Yale University

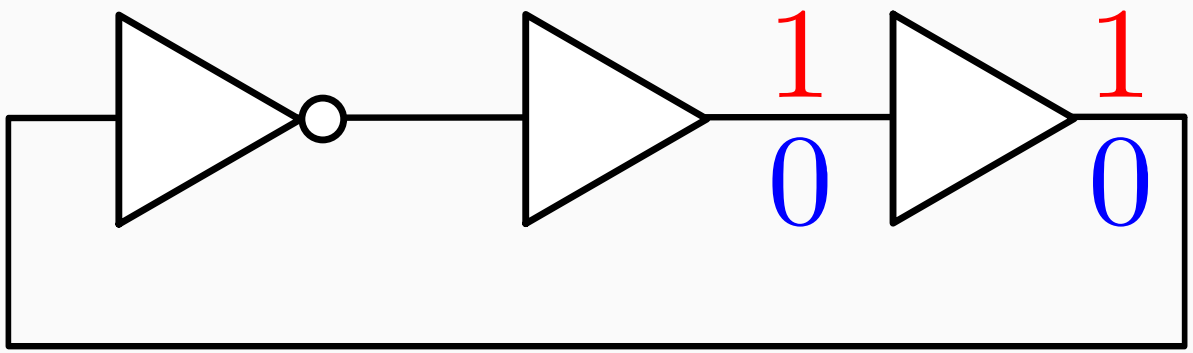
Cloud FPGAs

FPGAs now offered by cloud providers

- → Virtex UltraScale+ on Alibaba, **Amazon**, **Huawei**
- → Kintex UltraScale on Baidu, Tencent
- → Intel Arria 10 on Alibaba, OVH

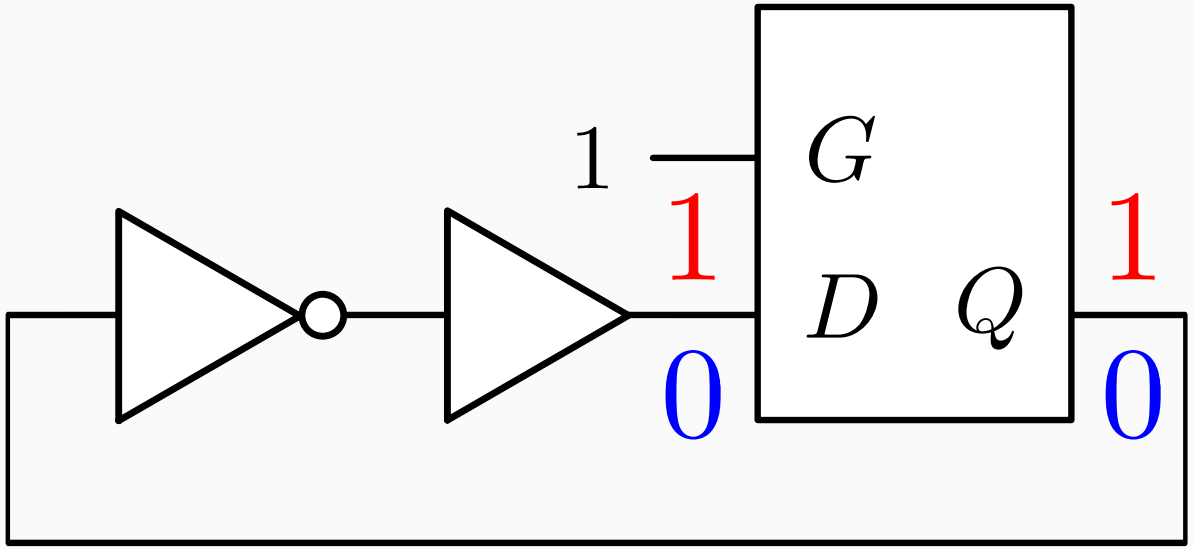
What about malicious designs?

- → Hide physical aspects (DRAM, PCIe, Clock, . . .)
- → Prohibit combinatorial loops (e.g., ring oscillators)



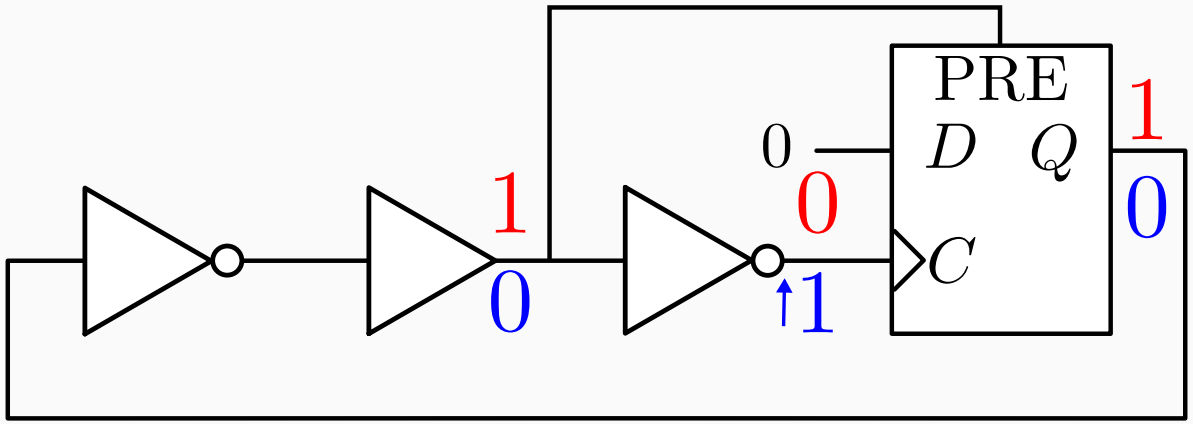
Latch-Based RO

Latches are level-sensitive, so they act as buffers: when the gate G is active, the output Q mirrors the input D.

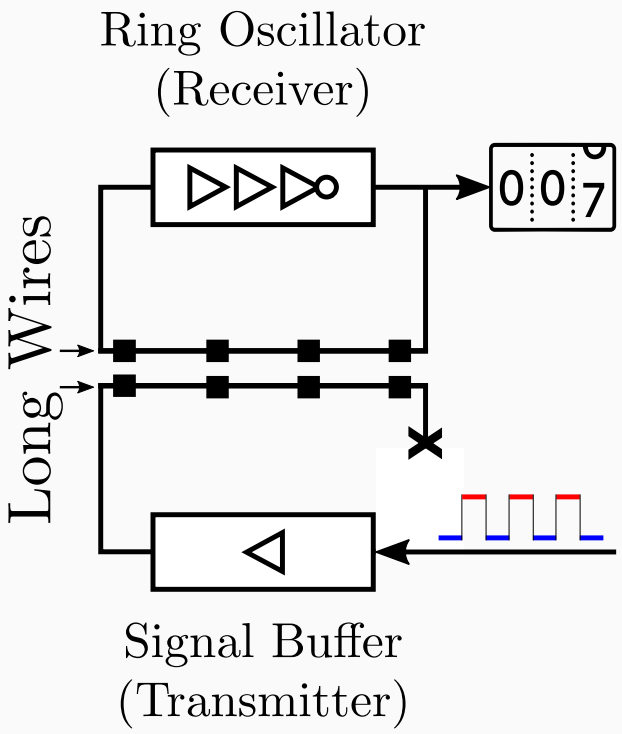


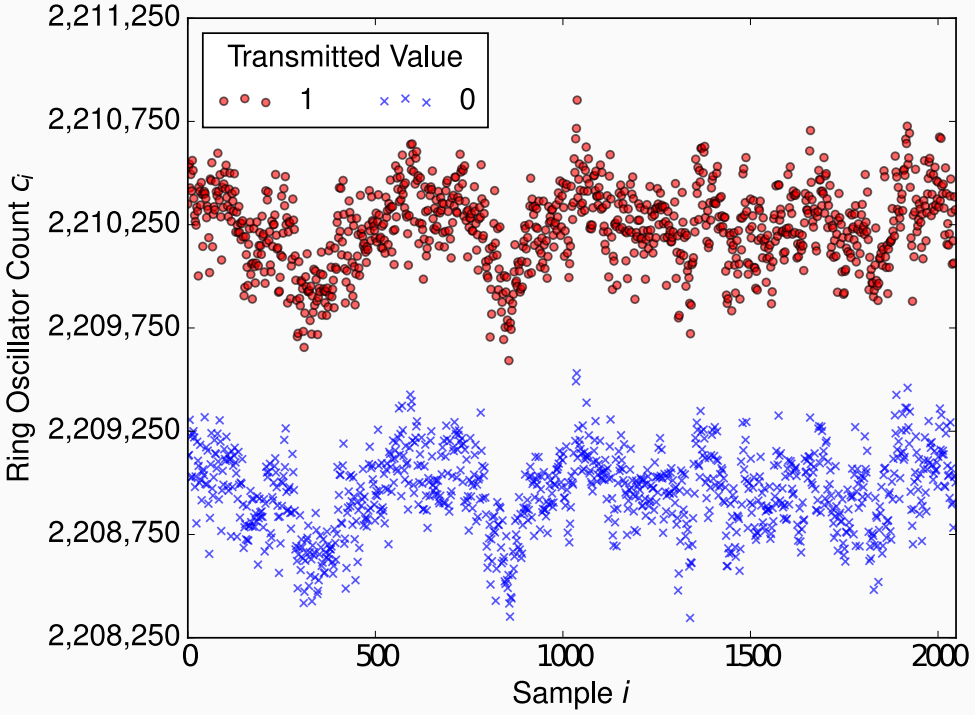
Flip-Flop-Based RO

For a flip-flop-based buffer, use a Flip-Flop with Asynchronous Preset *PRE*: when *PRE* is high, the output *Q* is also high. When the clock *C* rises, *Q* mirrors the input *D*.



Long Wire Leakage



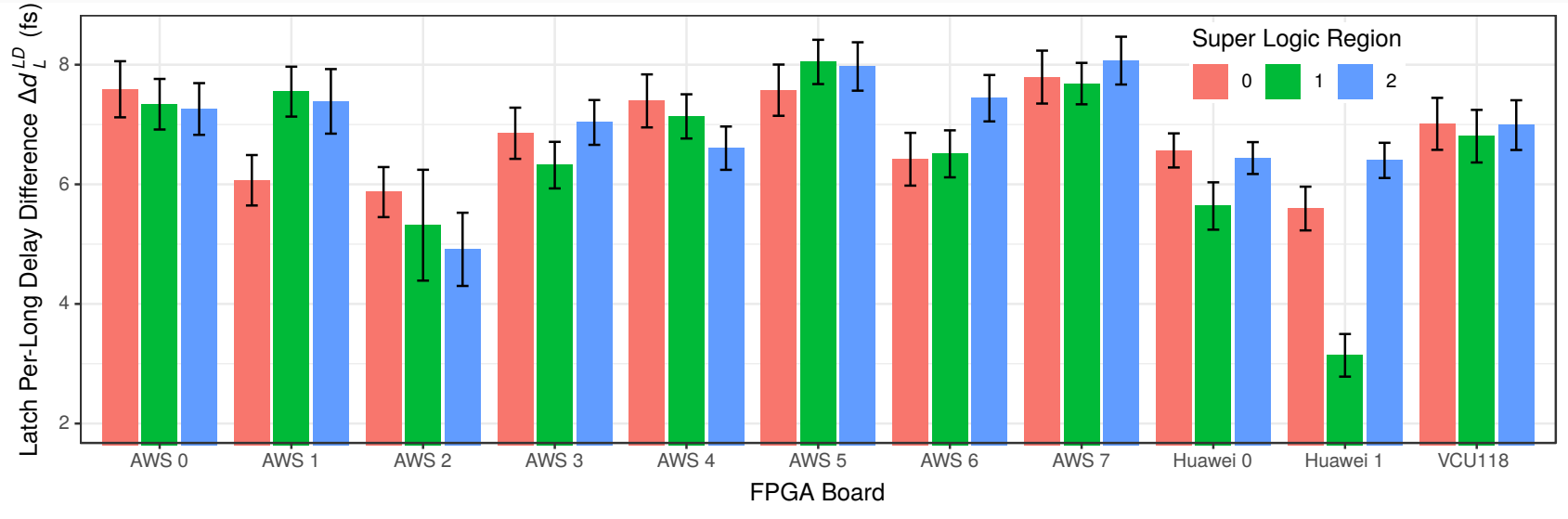


Earlier work: Virtex 5 & 6, Artix & Spartan 7 covert channels

This work: Virtex UltraScale+ leakage (on the cloud!)

Latch-Based Results

Experiments with 1 Local, 8 Amazon, 2 Huawei FPGAs



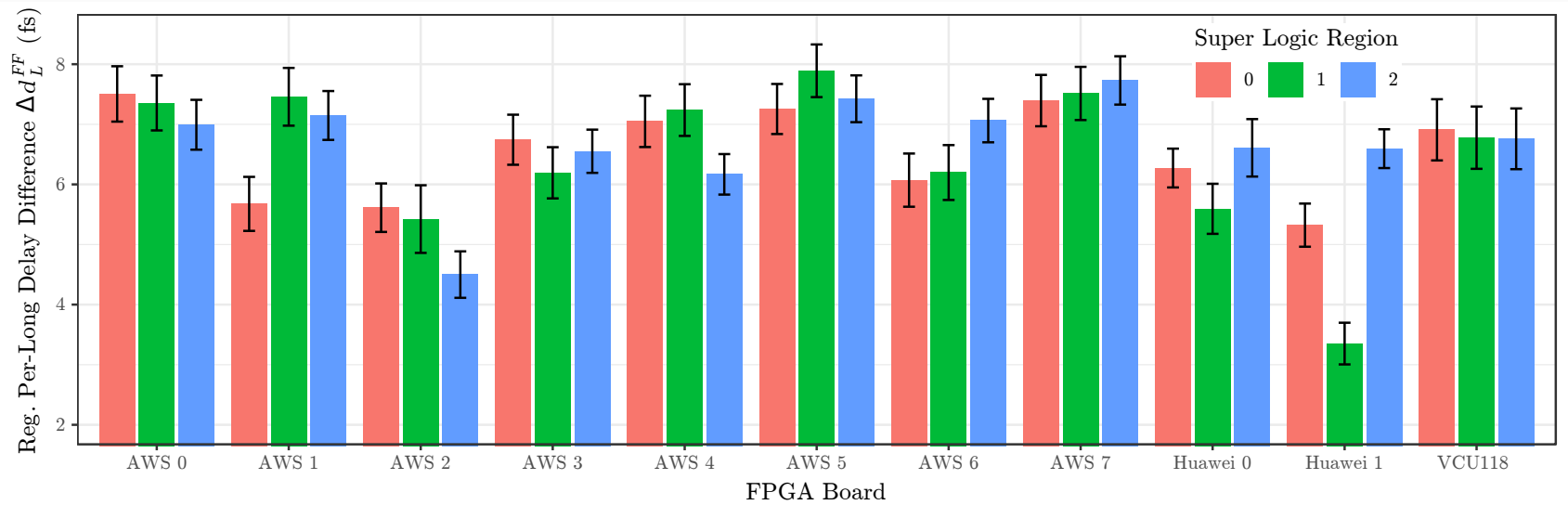
→ $\Delta d_L^{LD} > 0 \implies$ leakage detectable on all FPGAs

→ Process variations between FPGAs

→ Variations within FPGAs (between Super Logic Regions)

Flip-Flop-Based Results

Estimates with Flip-Flop ROs are very close::

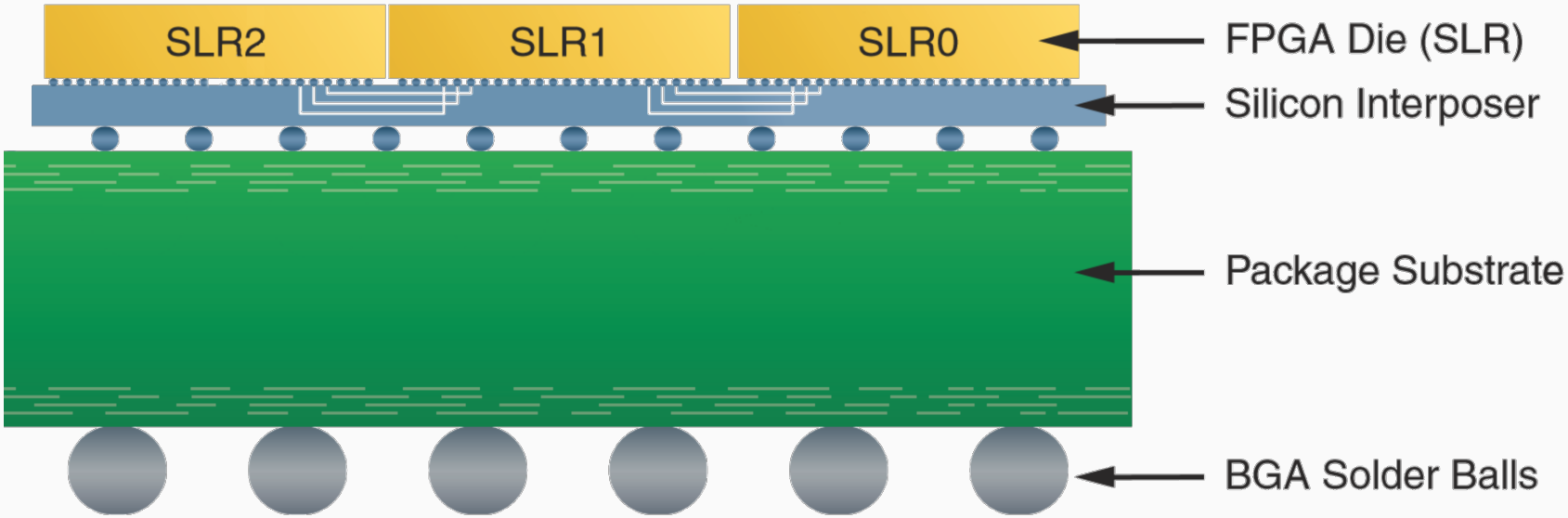


Same with Lookup-Table ROs (all within 10%)

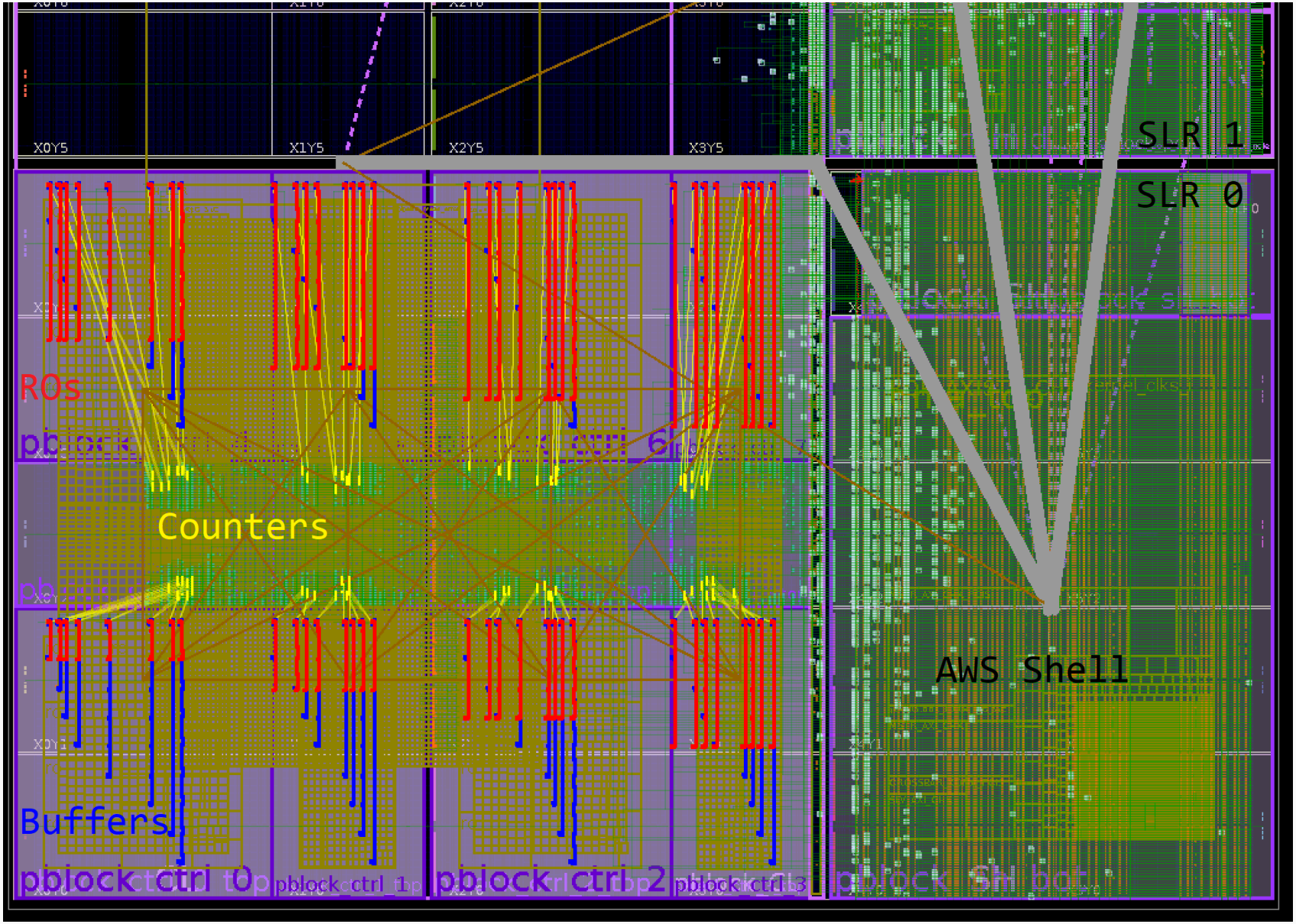
Conclusions

- → Latch-based and flip-flop-based ROs can overcome combinatorial loop restrictions
- → Virtex UltraScale+ FPGA long wires different from earlier generations, but still leak information about their state
- → The three RO designs provide identical leakage estimates
- → Comparison among 33 super logic regions in local, Amazon, and Huawei FPGAs revealed process variations
- → Questions? **ilias.giechaskiel@cs.ox.ac.uk**

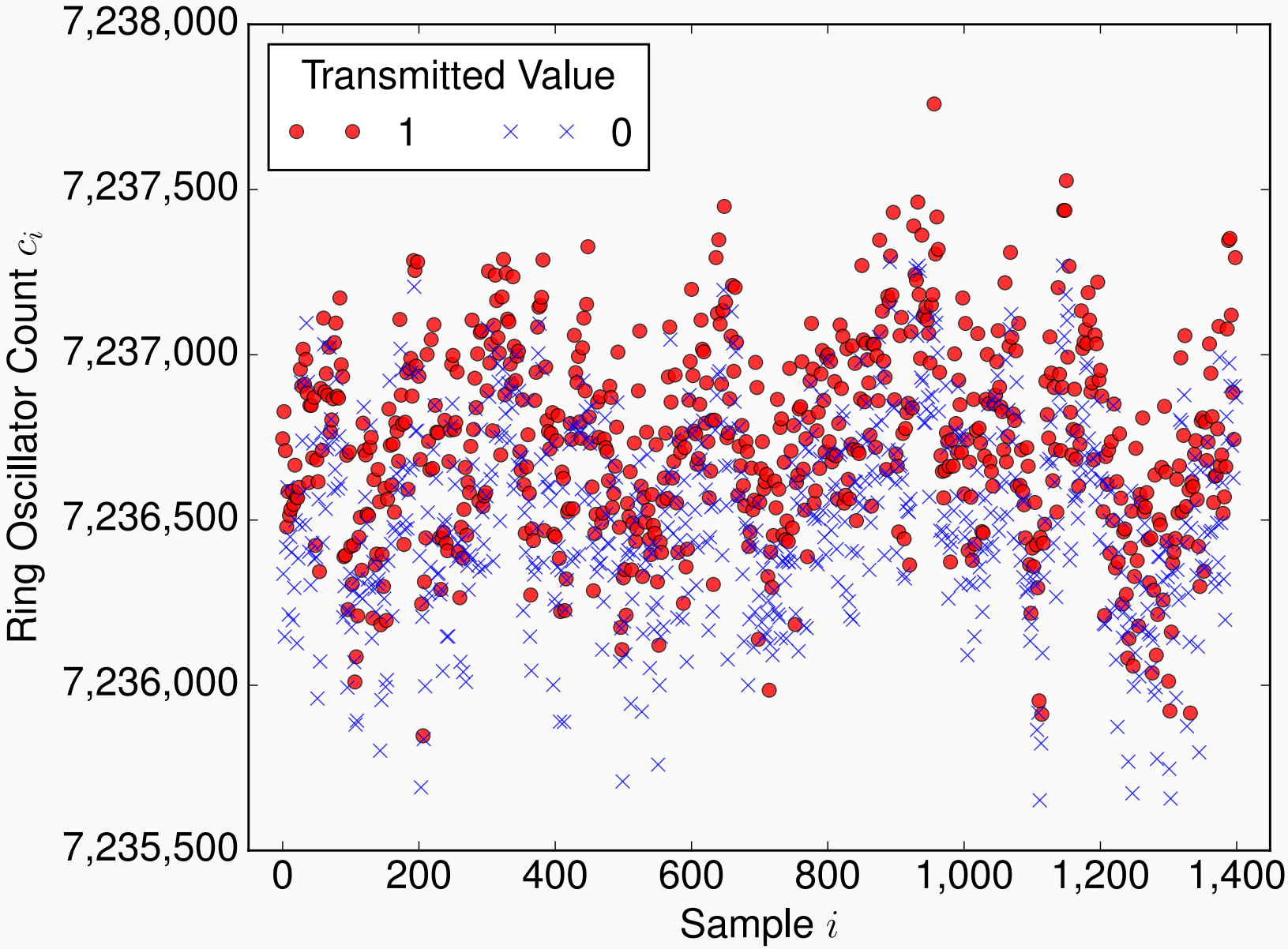
Super Logic Regions



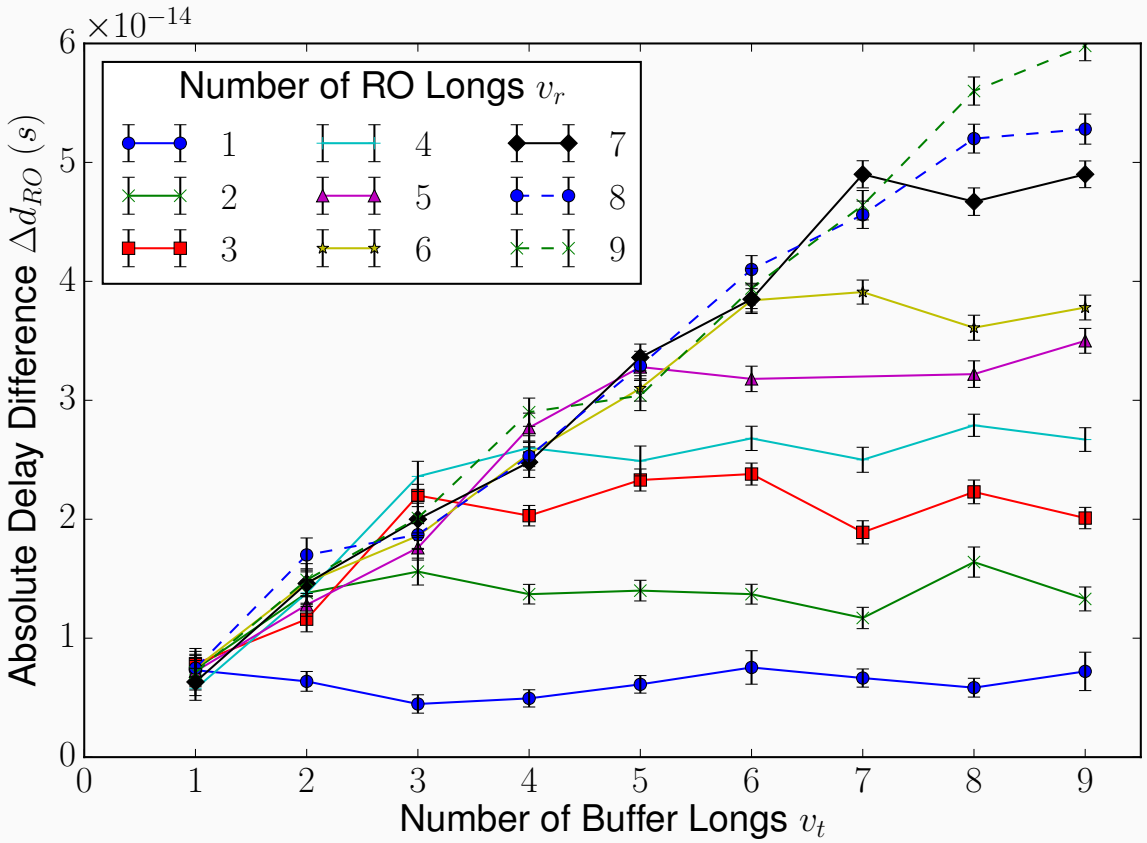
Routing Example



Virtex UltraScale+ Leakage Example

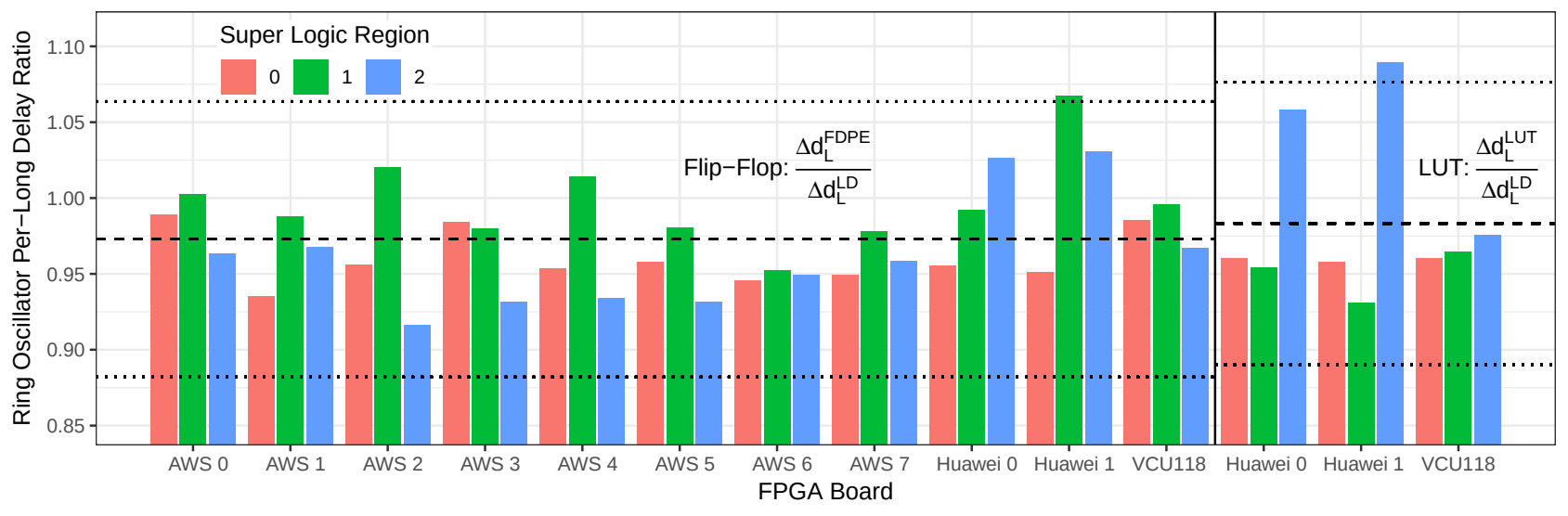


Virtex UltraScale+ Leakage Characterization



Femtosecond-scale change in delay is proportional to the overlap between the receiver and the transmitter

Flip-Flop- and Lookup-Table-Based Ratios



Property	Virtex 5	Virtex 6	Series 7	Virtex US+
Node Size (nm)	65	40	28	16
VLONG Length	18	16	18	12
VLONG Taps	2	1	1	0
VLONG Bidirectional?	✓	✓	✓	×
VLONGs/CLB	2	2	2	2×8

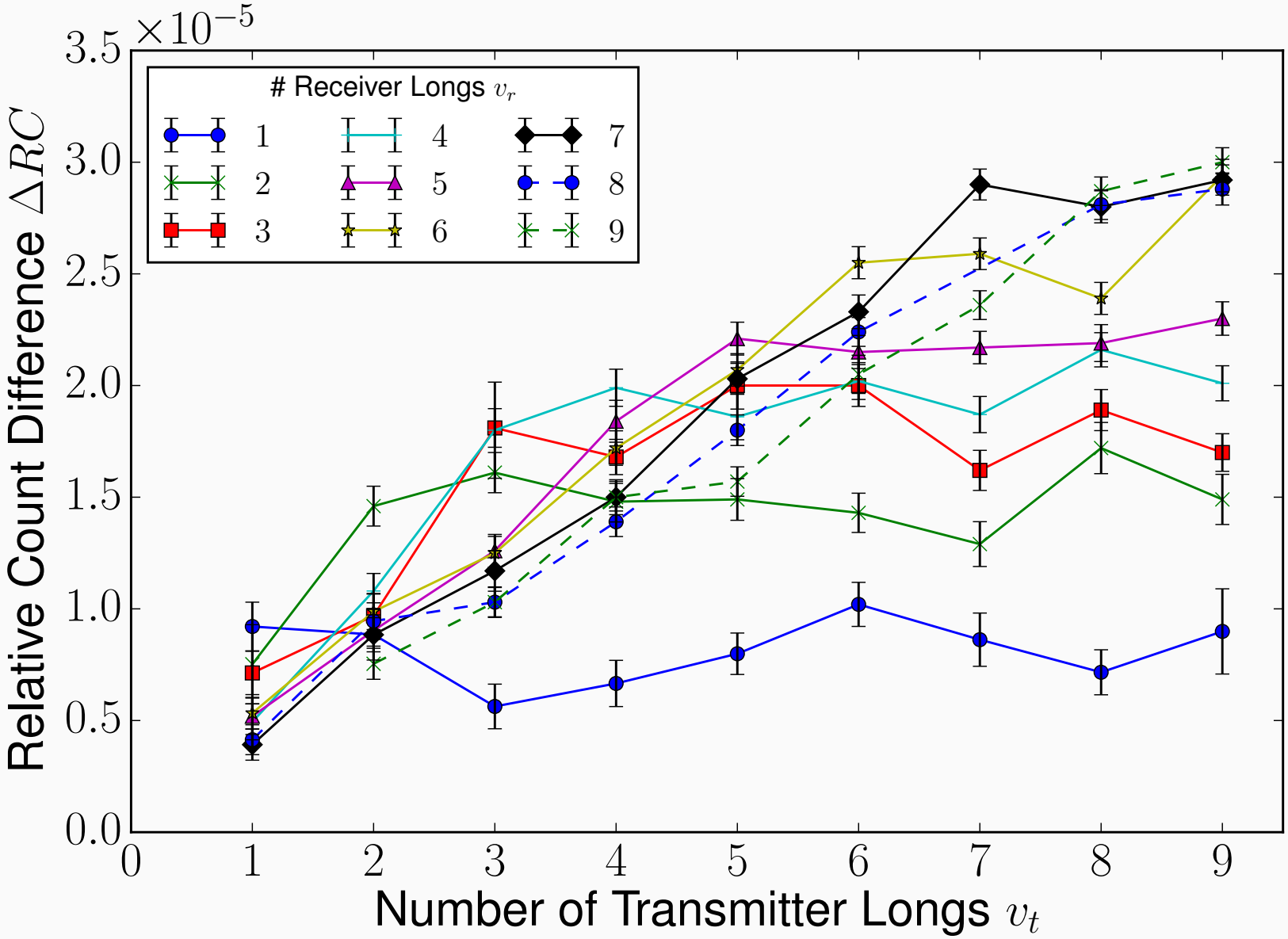
Metrics

$$\Delta RC = \frac{C_{RO}^{1} - C_{RO}^{0}}{C_{RO}^{1}} \tag{1}$$

$$\Delta d_{RO} = \frac{1}{2}\left(\frac{1}{f_{RO}^{0}} - \frac{1}{f_{RO}^{1}}\right) = \frac{f_{RO}^{1} - f_{RO}^{0}}{2 f_{RO}^{0} f_{RO}^{1}} \tag{2}$$

$$\Delta d_{L} = \frac{\Delta d_{RO}}{n} = \frac{1}{n} \cdot \frac{C_{CLK}}{2 f_{CLK}} \cdot \frac{C_{RO}^{1} - C_{RO}^{0}}{C_{RO}^{0} C_{RO}^{1}} \tag{3}$$

Relative Count Difference



Countermeasures

- → **Routing Restrictions:** Enforce physical isolation between users and potentially-malicious cores.
- → **Design Rule Checks:** Place restrictions on the generated bitstreams, including prohibiting combinatorial loops, latches, and non-shell clocks.
- → **Runtime Protections:** Gate clocks and clear the FPGA in response to detected malicious designs.