The Design and Analysis of a True Random Number Generator in an FPGA

Paul Kohlbrenner

Kris Gaj

February 24, 2004

Why Does Cryptographic Hardware Need Random Bits?

- Keys
- Initialization Vectors
- Challenges

Why are FPGAs Good Platforms for Crypto Systems?

Category	ASICs	FPGAs	Software
Speed	3	2	1
Development Cost	1	2	3
Development Time	1	2	3
Cost of Development Tools	1	3	3
Tamper Resistance	3	2	1
Key Protection	3	2	1
Algorithm Agility	1	3	3
Random Number Generation	3	1	1
Totals:	16	17	16

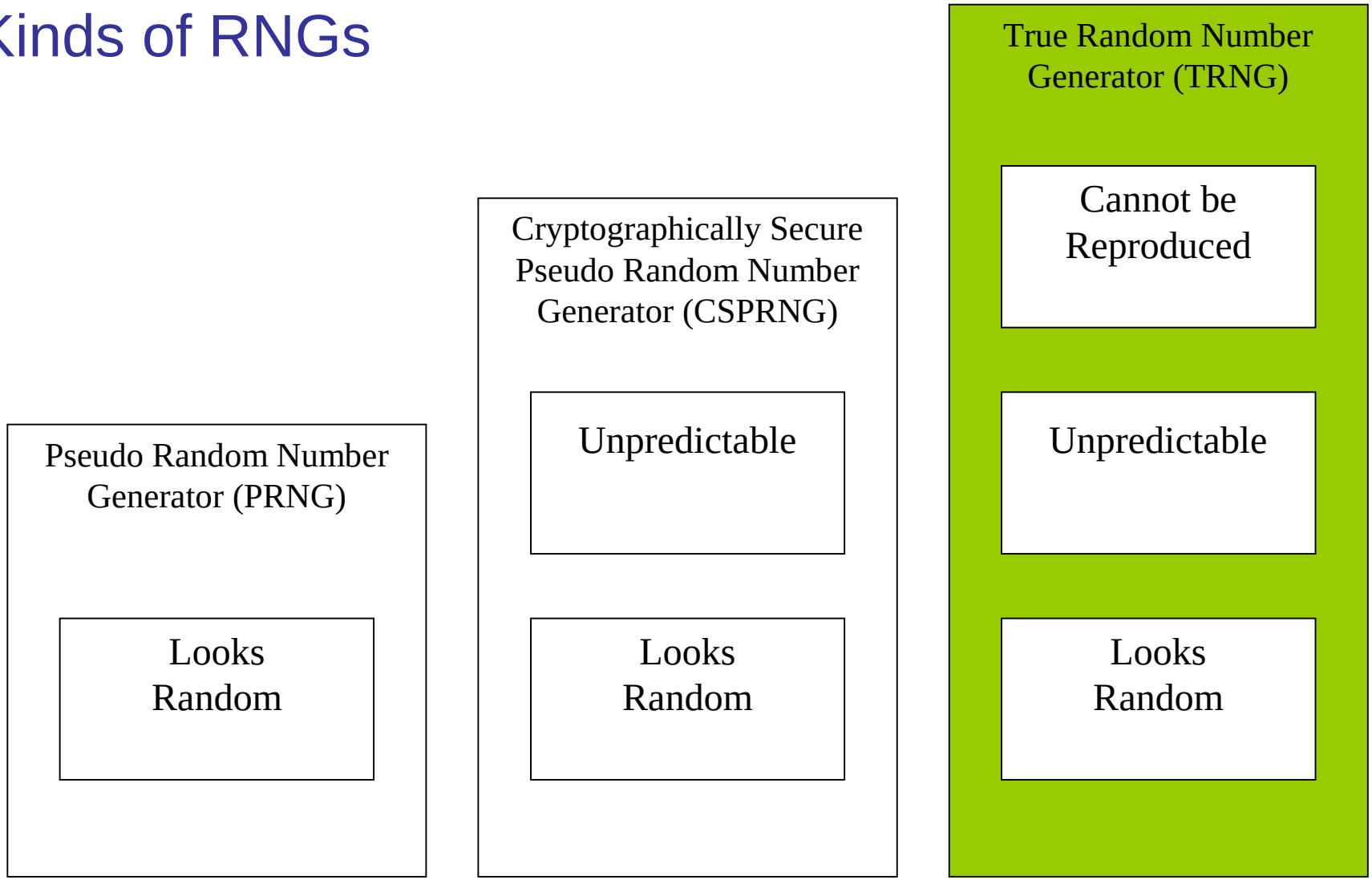
What is a Random Number Generator?

Working definition (from Bruce Schneier):

The Output:

1. Looks random (passes statistical tests).
2. Is unpredictable.
3. Cannot be reproduced.

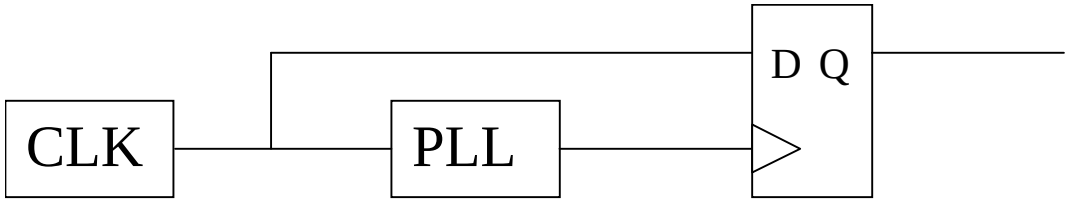
Kinds of RNGs



Previous Work

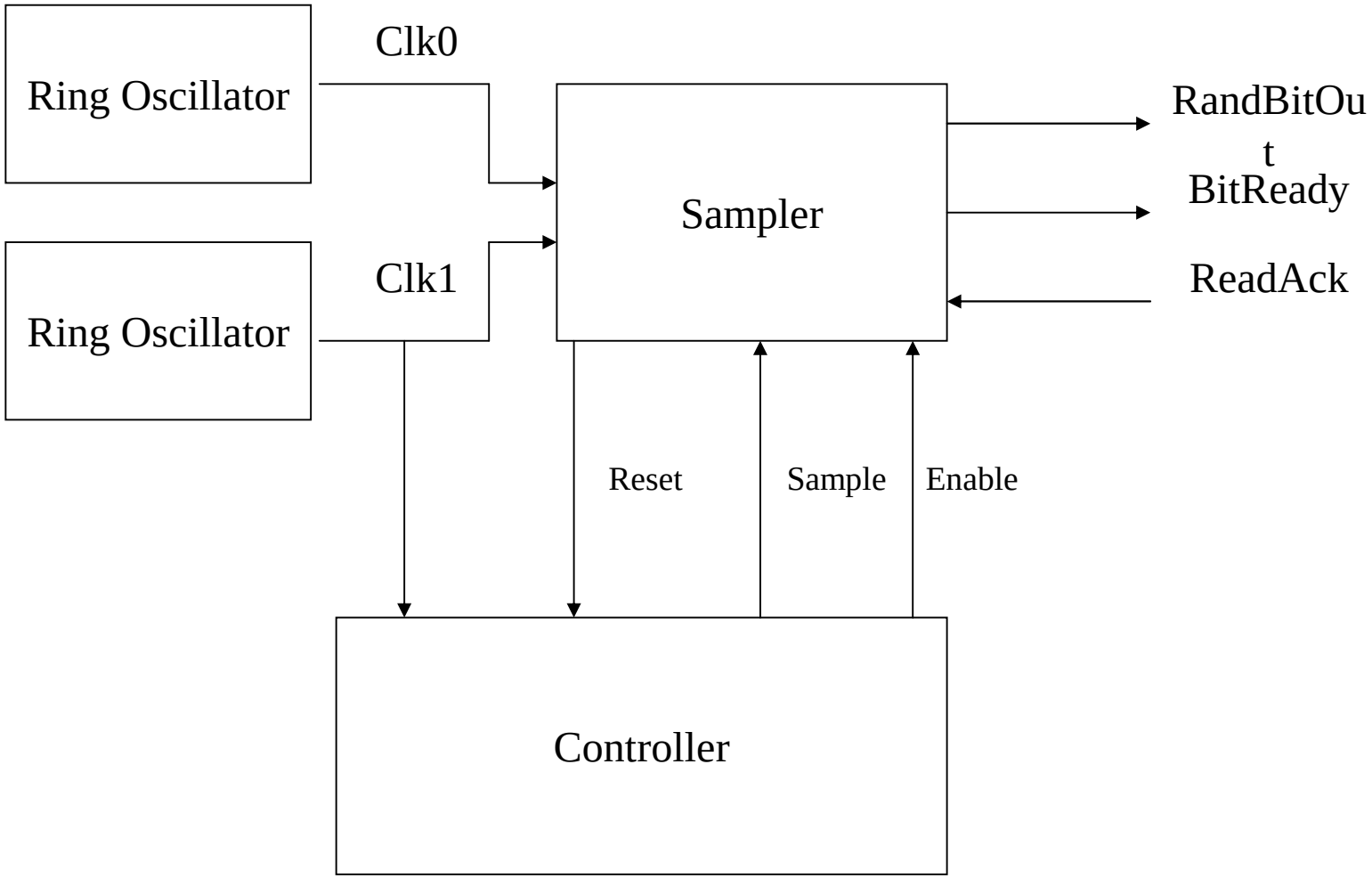
- Fischer & Drutarovský (CHES 2002):

  TRNG for FPGAs containing PLLs (e.g. Altera)

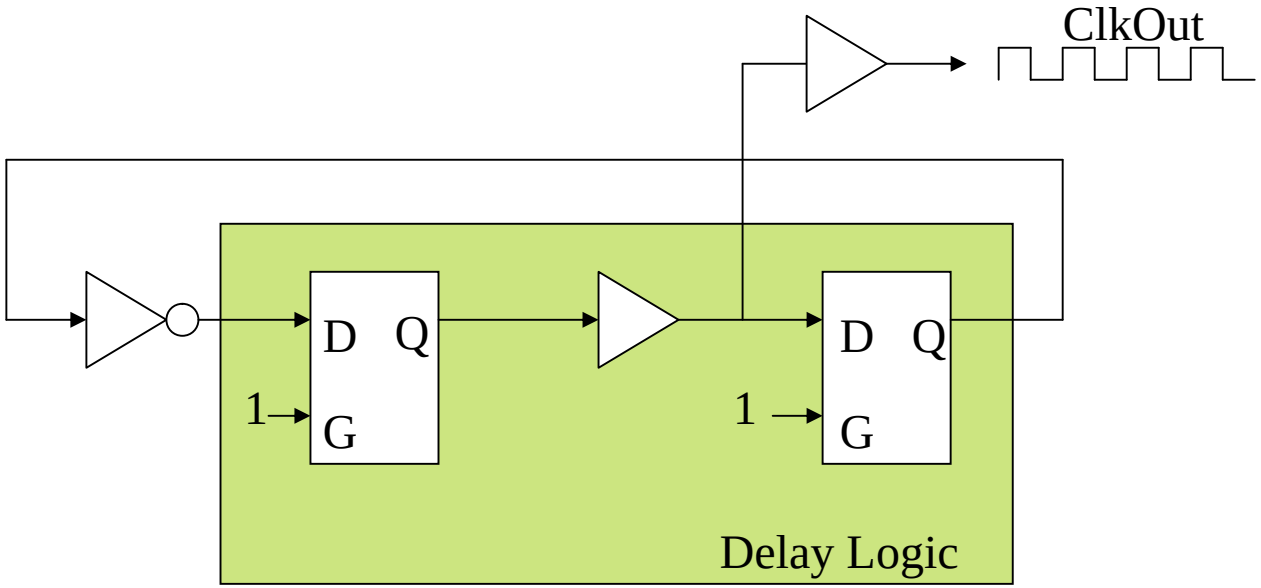


  Cannot be implemented with DLLs used in many FPGAs (e.g. Xilinx) because DLLs do not allow fine enough control over frequency synthesis.

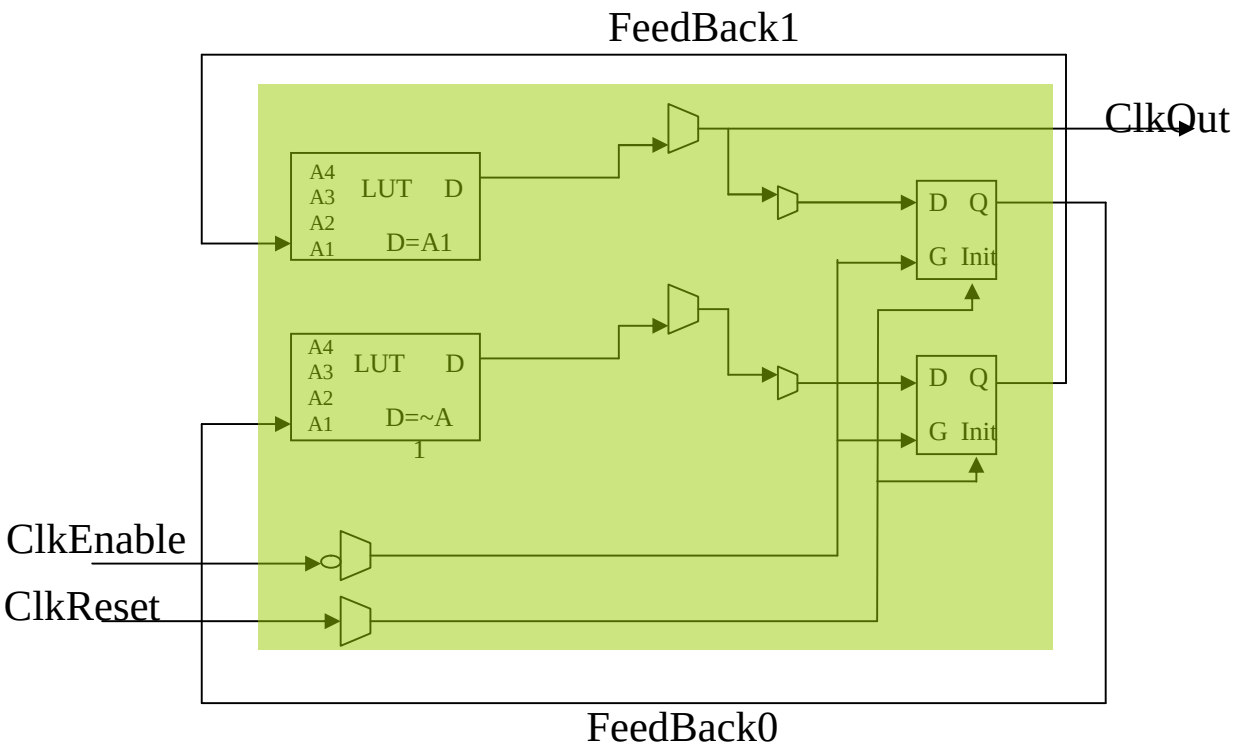
Our Design - Overview



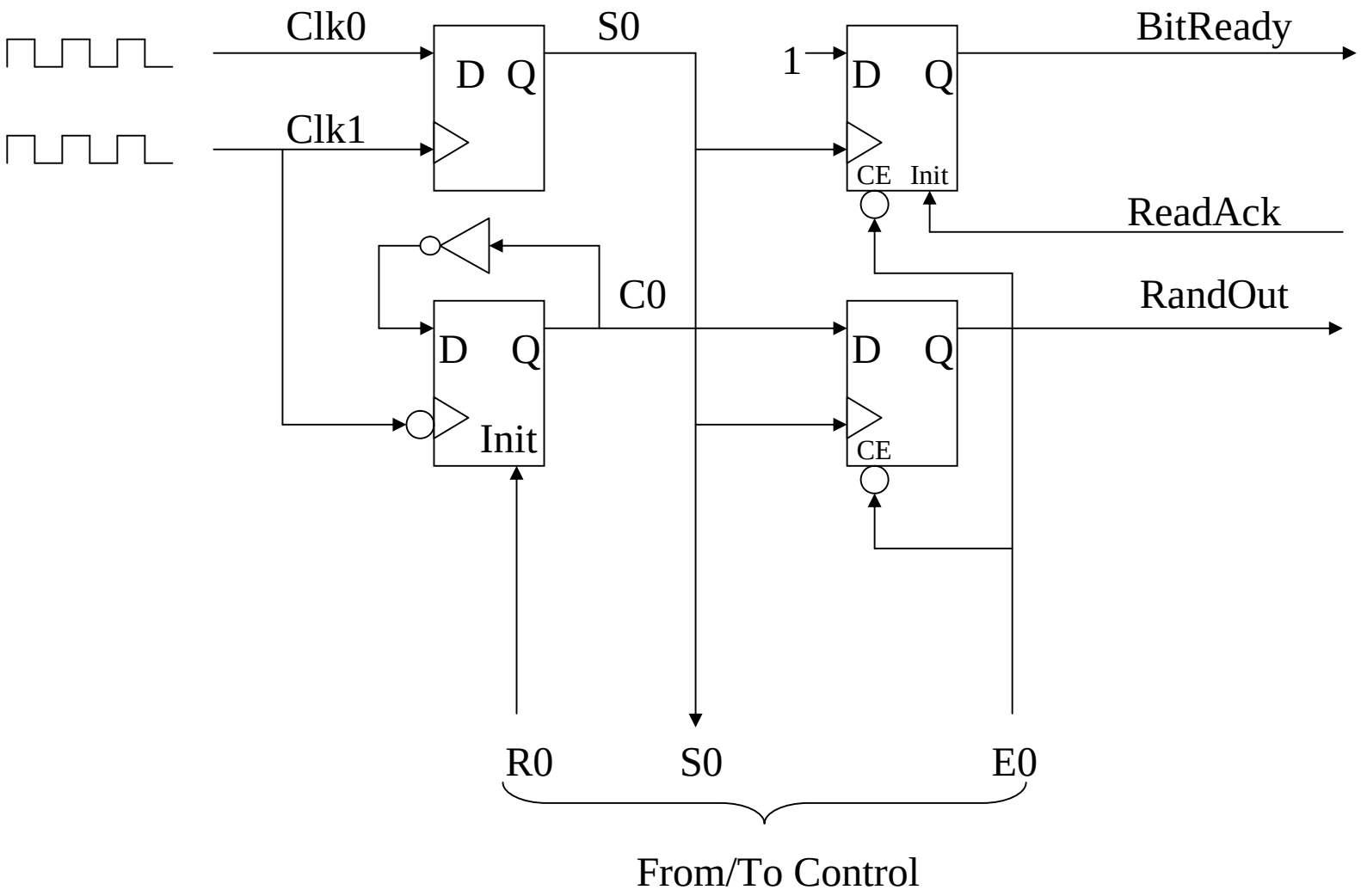
Our Design for Xilinx FPGAs – The Ring Oscillators



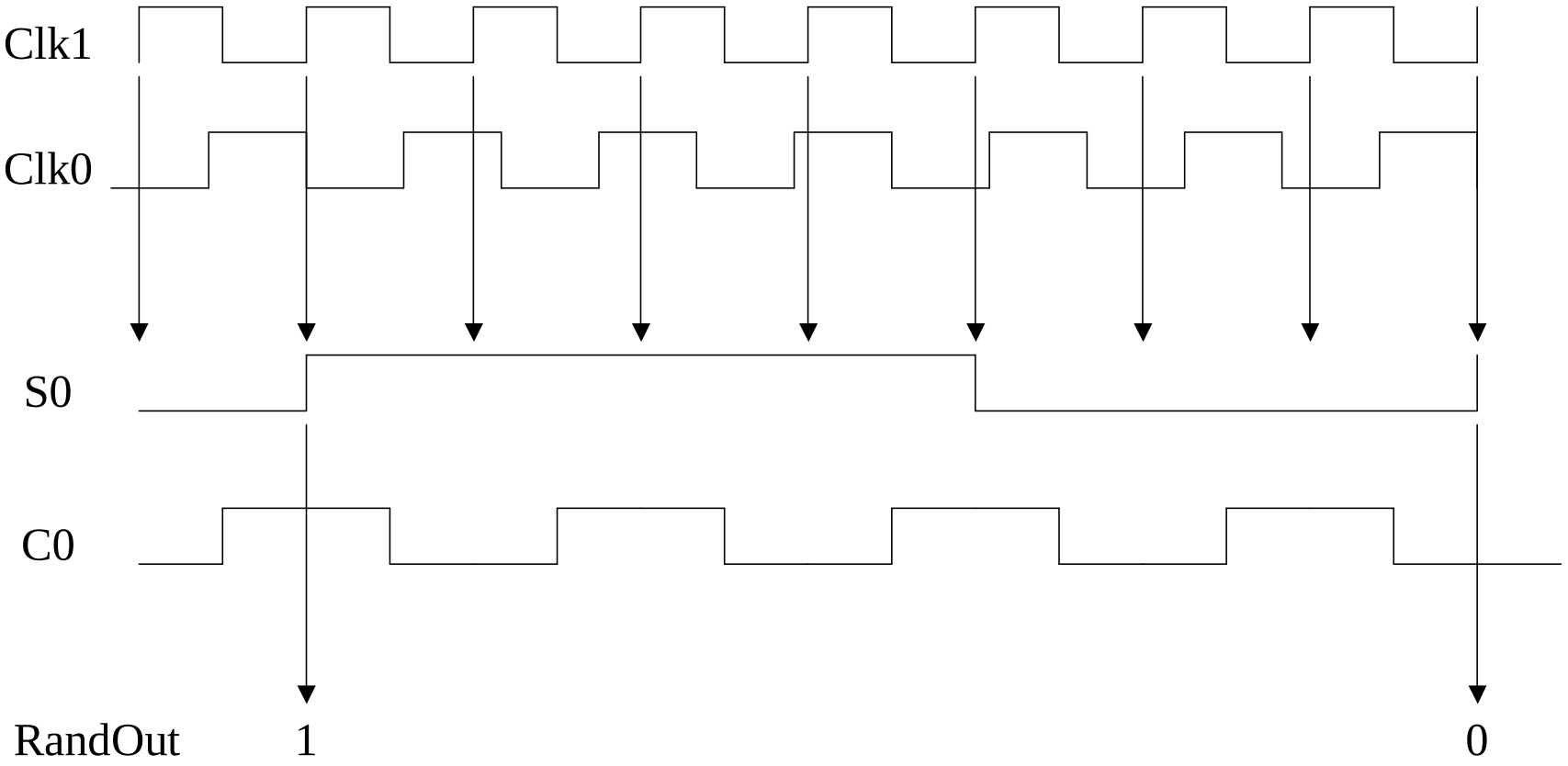
Our Design for Xilinx FPGAs – The Ring Oscillators



Our Design for Xilinx FPGAs – The Sampler



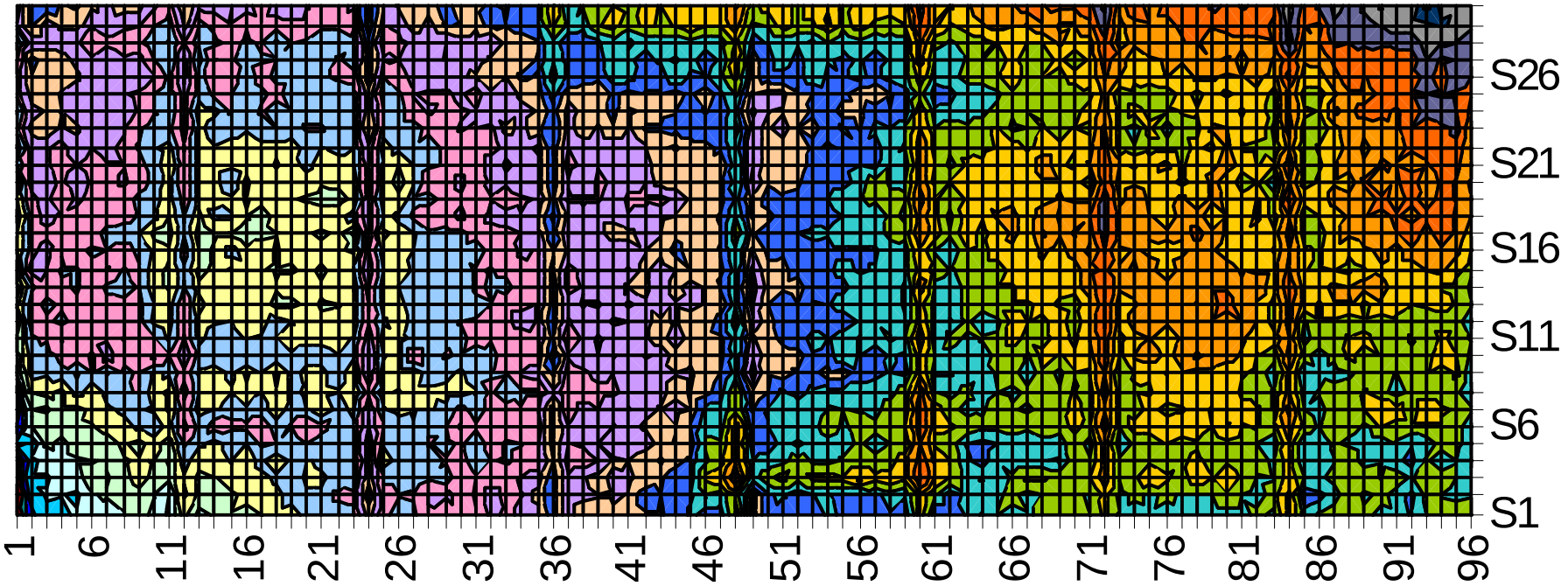
Our Design for Xilinx FPGAs – Sampler Operation



Our Design for Xilinx FPGAs – Advanced Features

- Control circuit inhibits output if S0 signal not long enough to contain a random bit.

Our Design – More Ring Oscillators

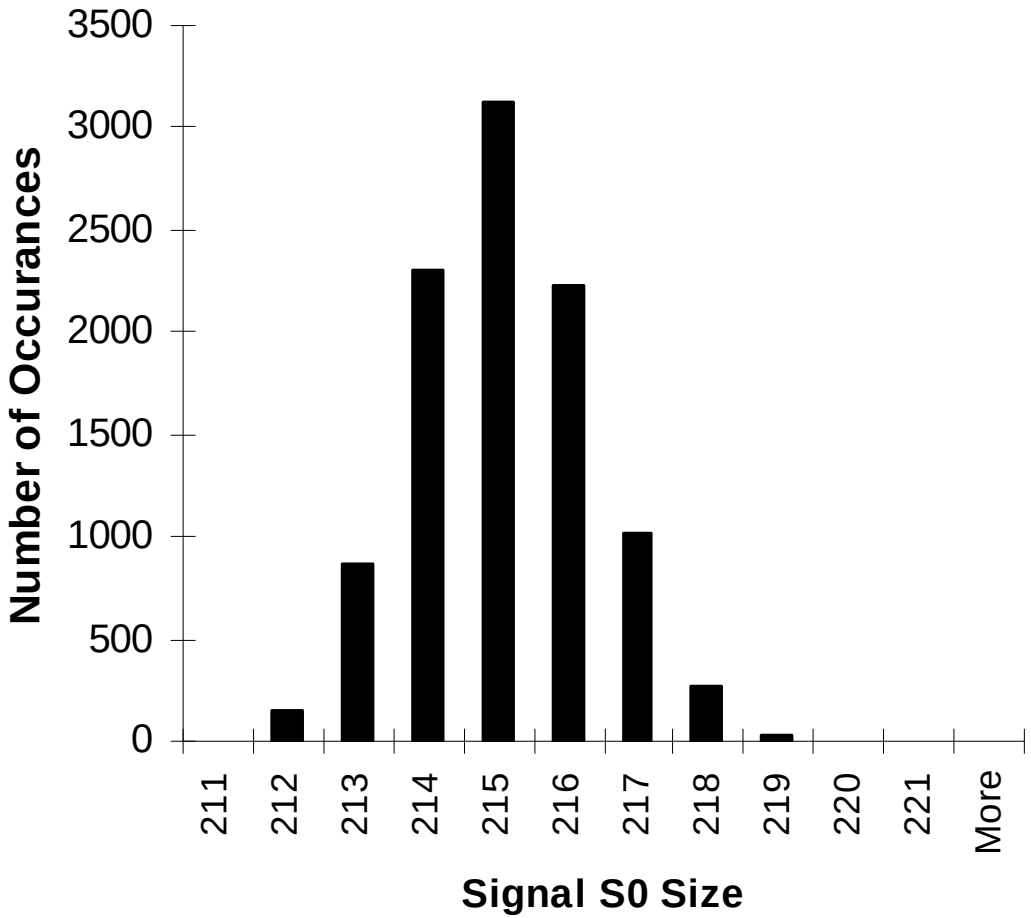


Our Design – Evidence of Jitter

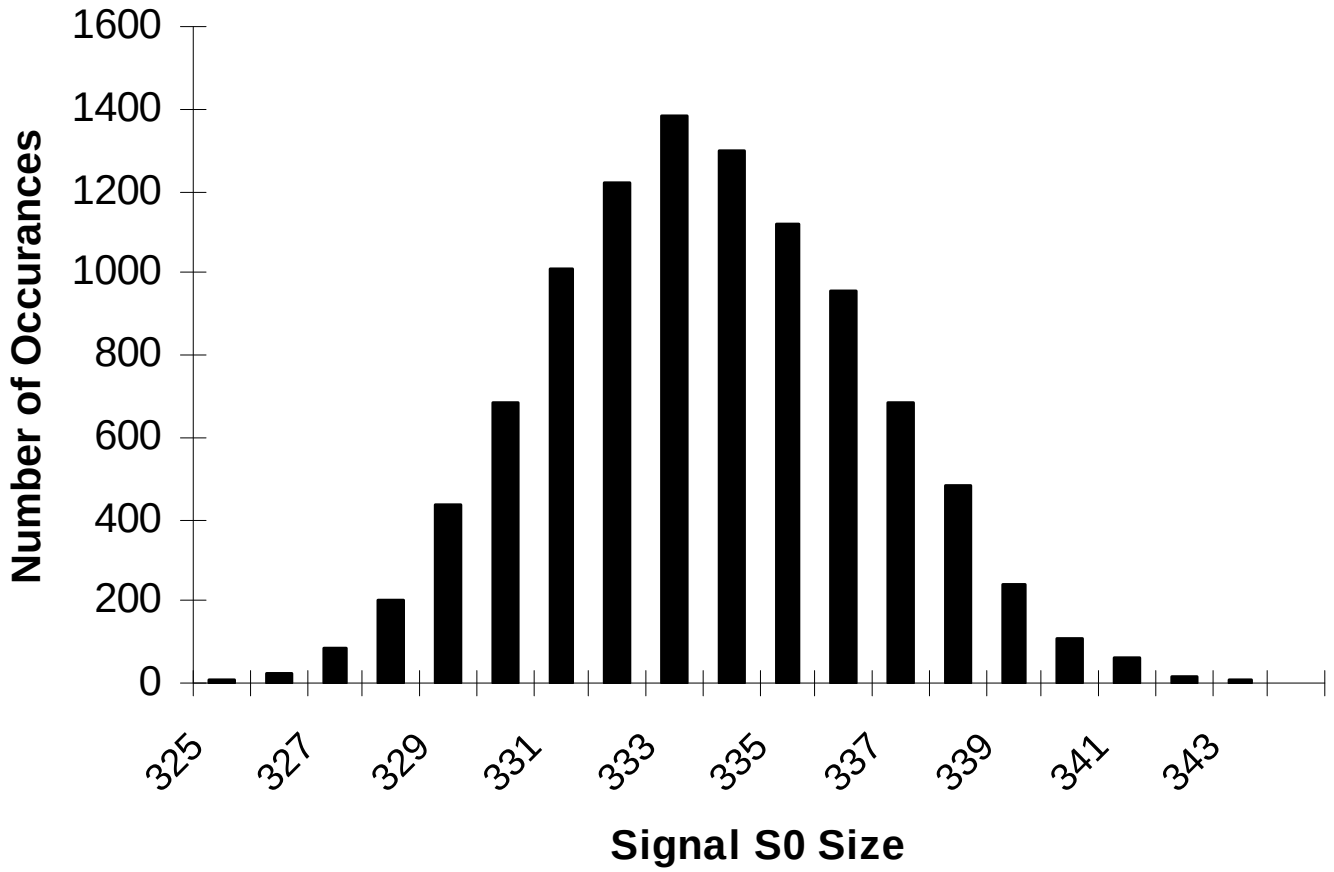
Experiment

- Add a counter to the clk0 signal and latch the count every time a random bit is output.
- If there is no jitter then the count will always be at most two different values.

Our Design – Evidence of Jitter



Our Design – Evidence of Jitter



Testing RNGs

- Use a variety of statistical tests to examine the output to make sure it meets the desired characteristics.
- (TRNGs only) Make sure the physical source of randomness is functioning.
- Two widely used public domain test suites:
  - DIEHARD
  - NIST

Future Work

- I created a design that used one CLK1 signal sampling four CLK0s. Initial tests showed that out of 78 placements across the top half of the FPGA only four failed to produce initial evidence of randomness.
- Slower ring oscillators might produce wider tolerances for oscillator differences.

Questions