PHILIPS

Design and Implementation of a True Random Number Generator Based on Digital Circuit Artifacts

Michael Epstein, Laszlo Hars, Raymond Krasinski,
Martin Rosner, Hao Zheng

September 9, 2003

Outline

- Description of randomness
- Digital circuit artifacts
  - Meta-stability
  - Jitter
- A practical random number generator
- Prototype measurements
- Conclusion

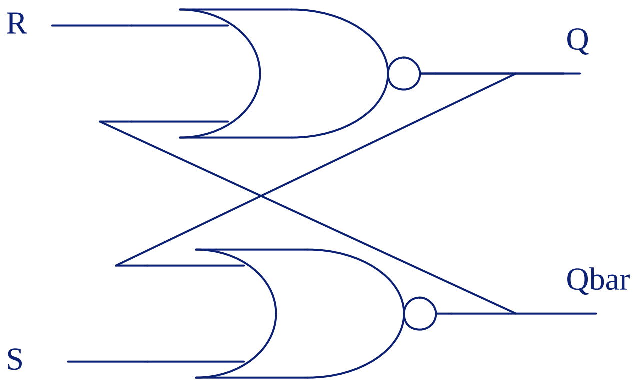
What is Real Randomness?

- Statistical uniformity
  - Unbiased - 50% of the bits are ones and 50% are zeros
  - Fairness, all sequences are equally likely
- Knowing the past gives no hint of the future
- Derived from physical phenomena
  - Radioactive source
  - Thermal noise
  - Cannot be predicted, because no one has been able to predict it yet!
- Common Problems
  - Complex circuits
  - Physical/circuit size

Premise: Get Randomness from a Digital Circuit

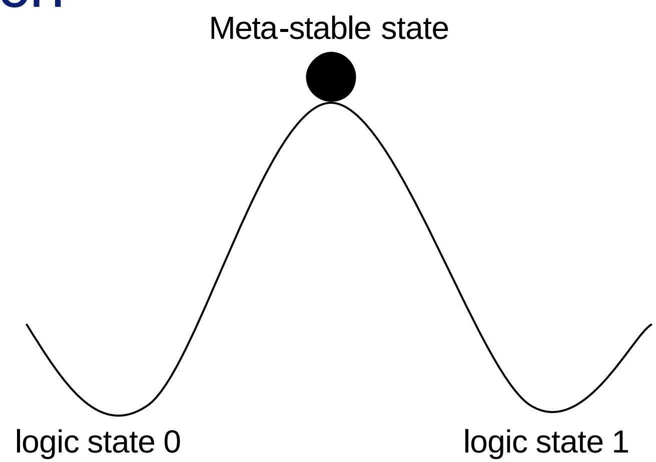
- But the output of any digital circuit is always predictable (when used properly)
  - Digital circuits only manipulate bits
  - Every bit is absolute i.e. it is a one or a zero
  - Given known inputs the output is always the same
    - Ignore pseudo-randomness (that is cheating and all papers on the topic are about when you get caught)
- Suggestion: Do not use the circuit as intended
  - Poor circuit models but **RANDOM BEHAVIOR**

Meta-stability

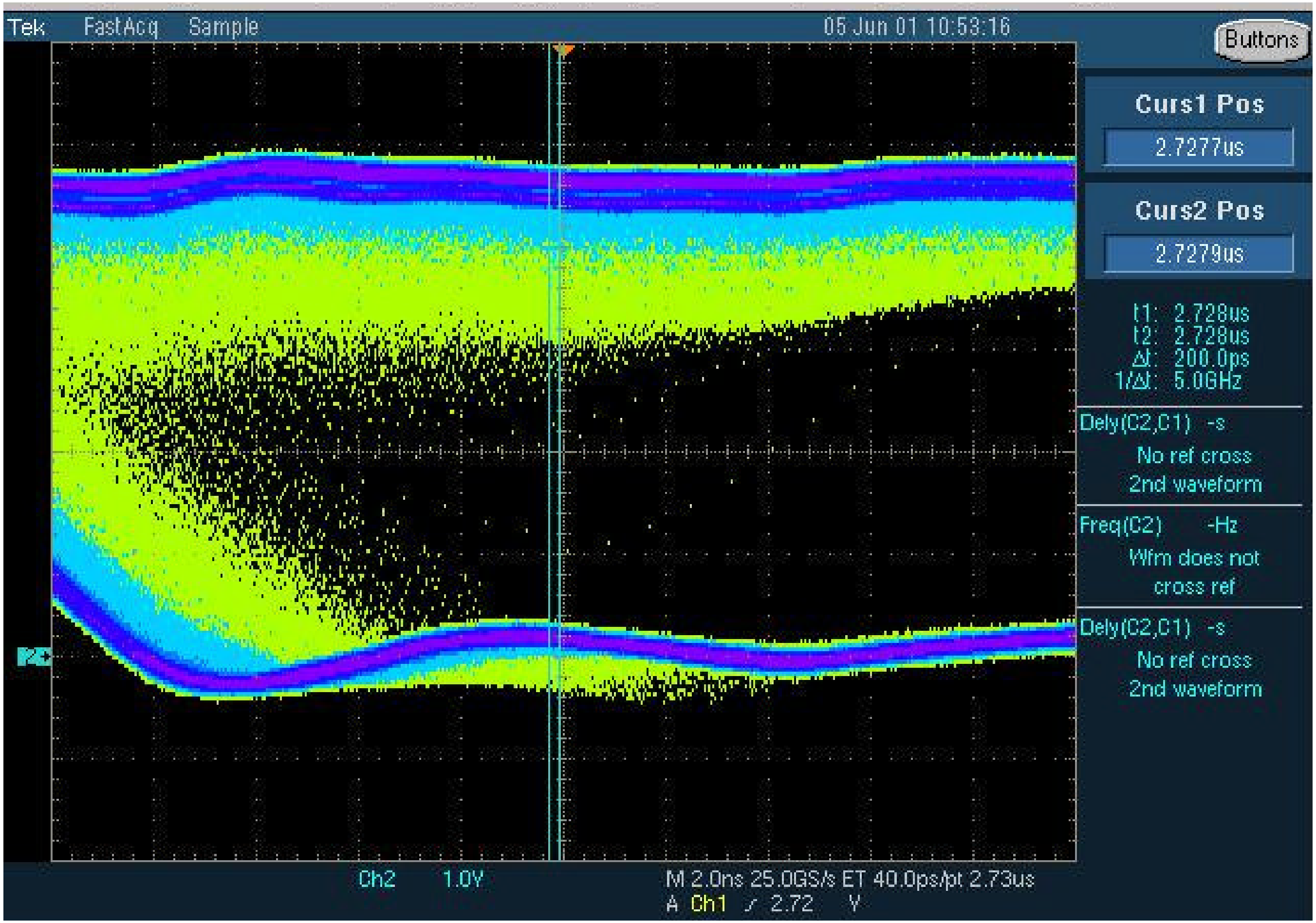


Set/Reset Latch

S	R	Q	Qbar	Comment
1	0	1	0	set
0	0	1	0	stable
0	1	0	1	reset
0	0	0	1	stable
1	1	0	0	abnormal
0	0	X	X	meta-stable

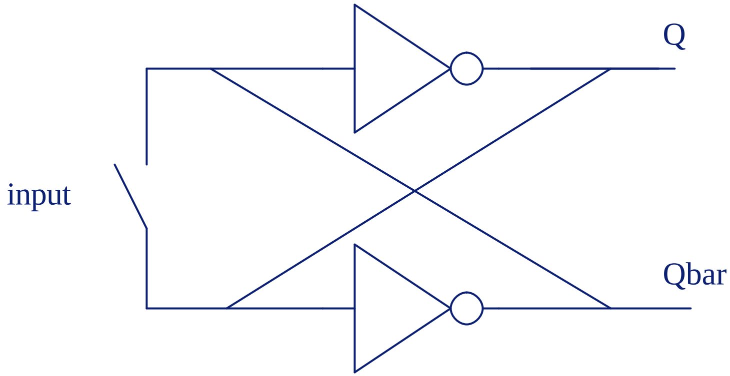


Breadboard Result

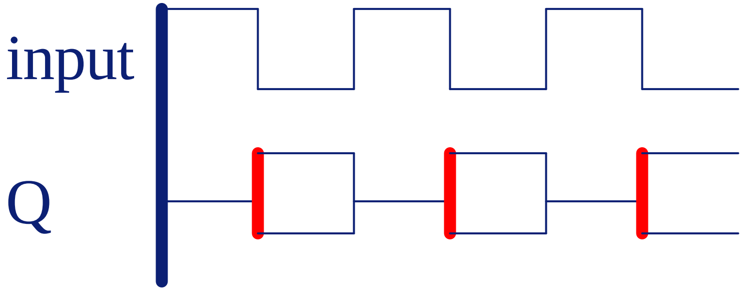


Flip-flop metastability on Oscilloscope

Previous Work



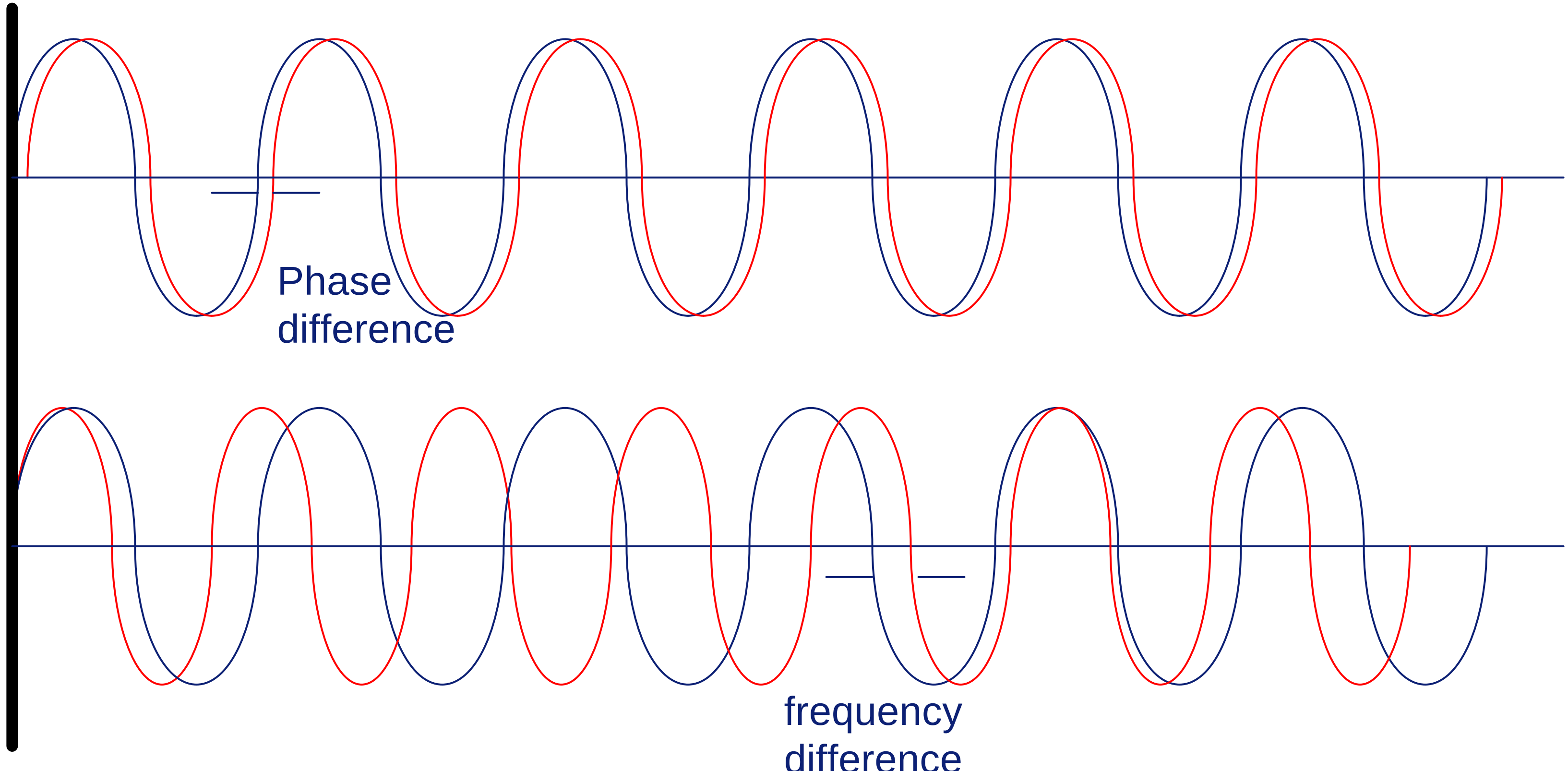
input	Q	Qbar	comment
1	N	N	neutral
0	X	X	meta-stable



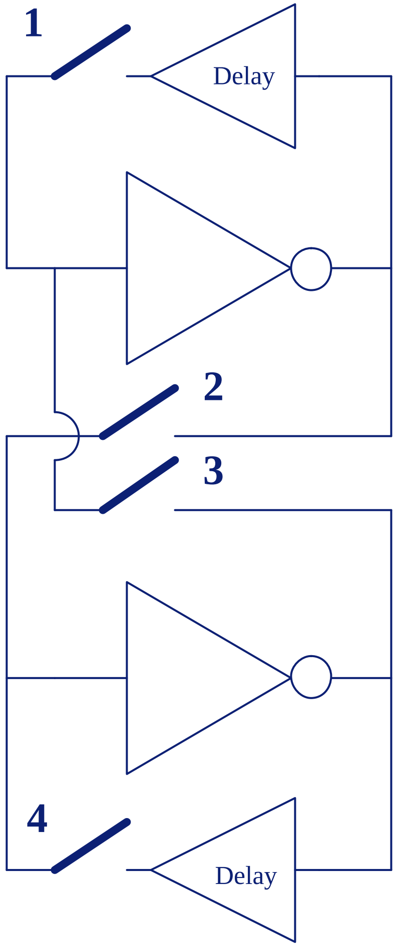
- M.J. Bellido, A.J. Acosta, et al. published in 1992
- Output is biased except under controlled conditions
  - Laser trimmed device
- phenomena was replicated with a relay or mechanical switch

Jitter

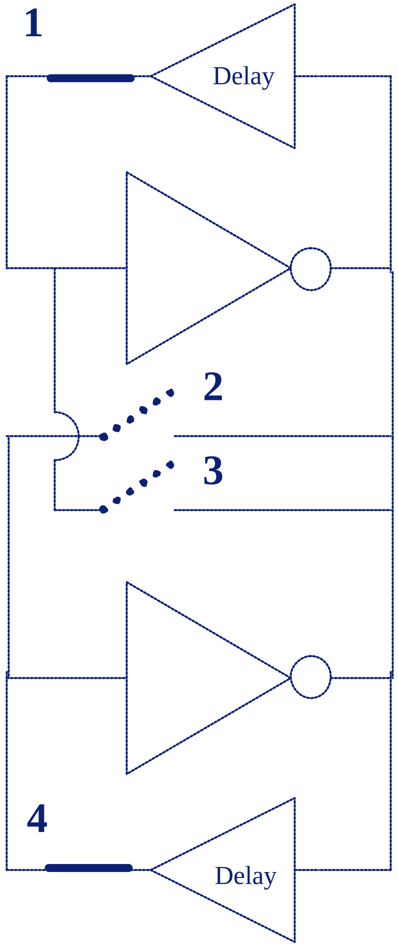
- Uncertainty about phase and/or frequency of a repetitive signal
  - Patterned components
  - Random components



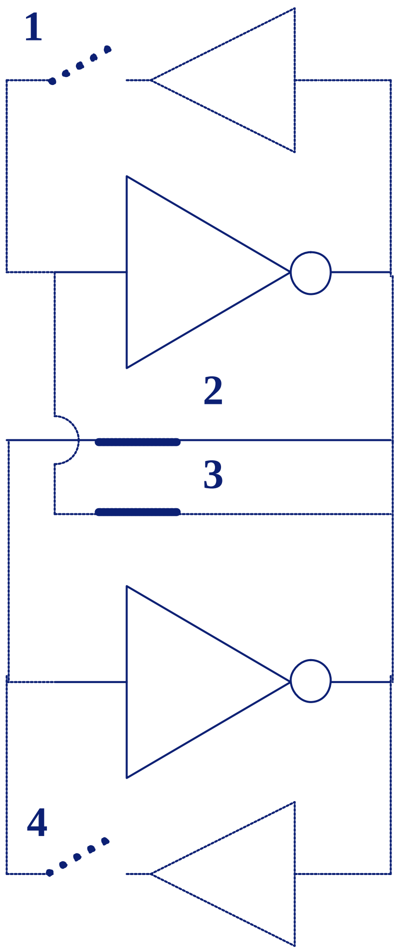
The Four Switch Solution



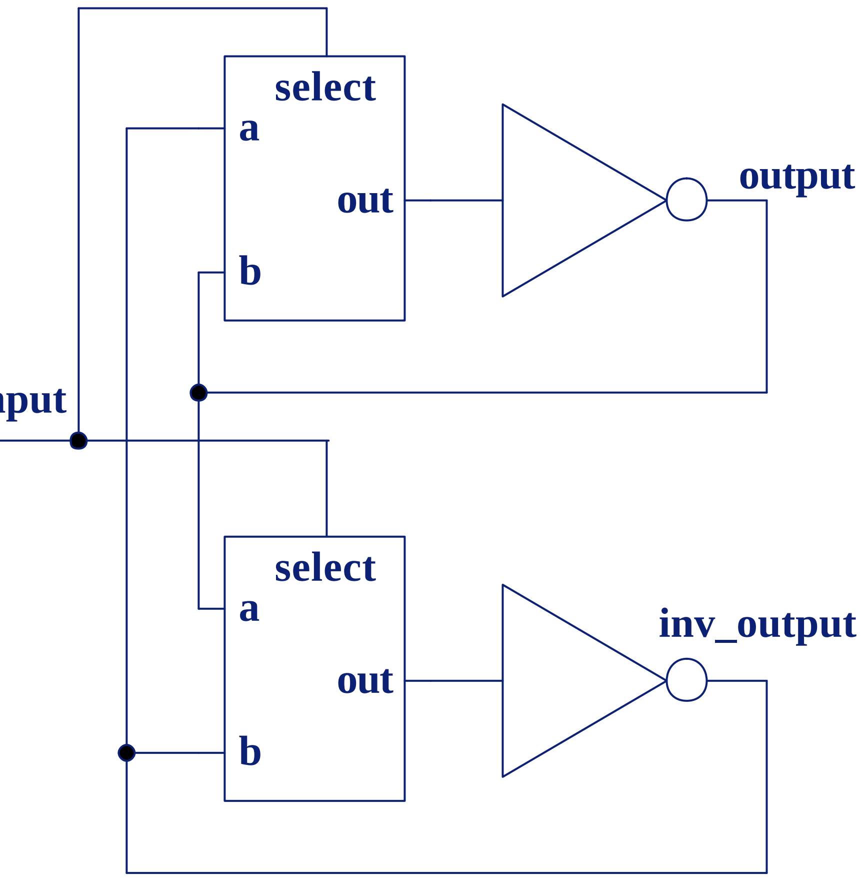
Oscillator Mode

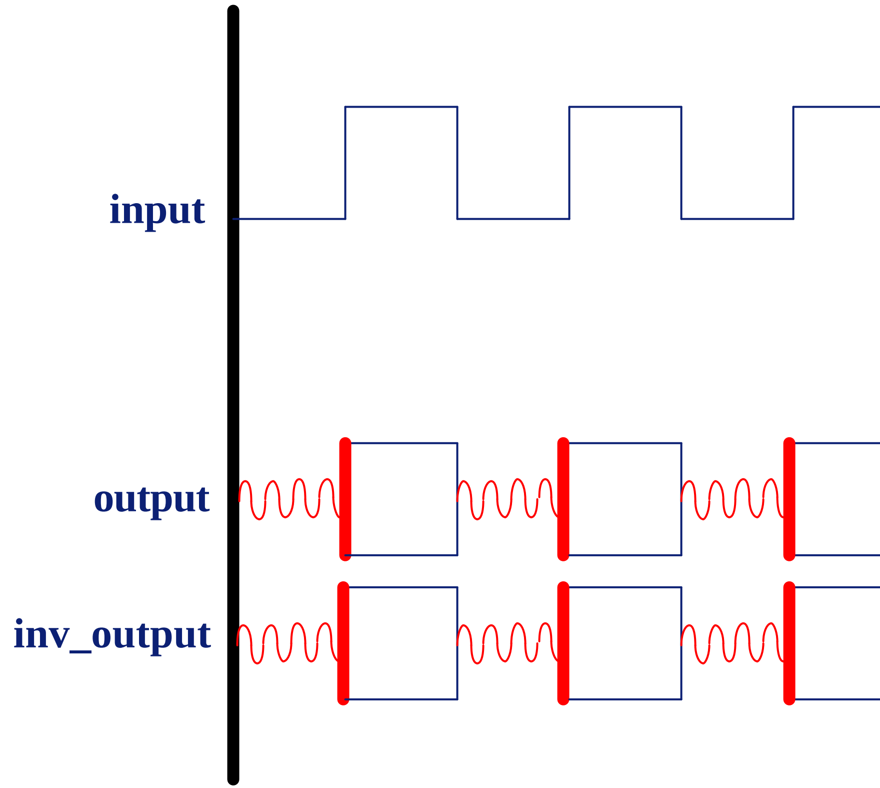


Resolve mode



Silicon Implementation





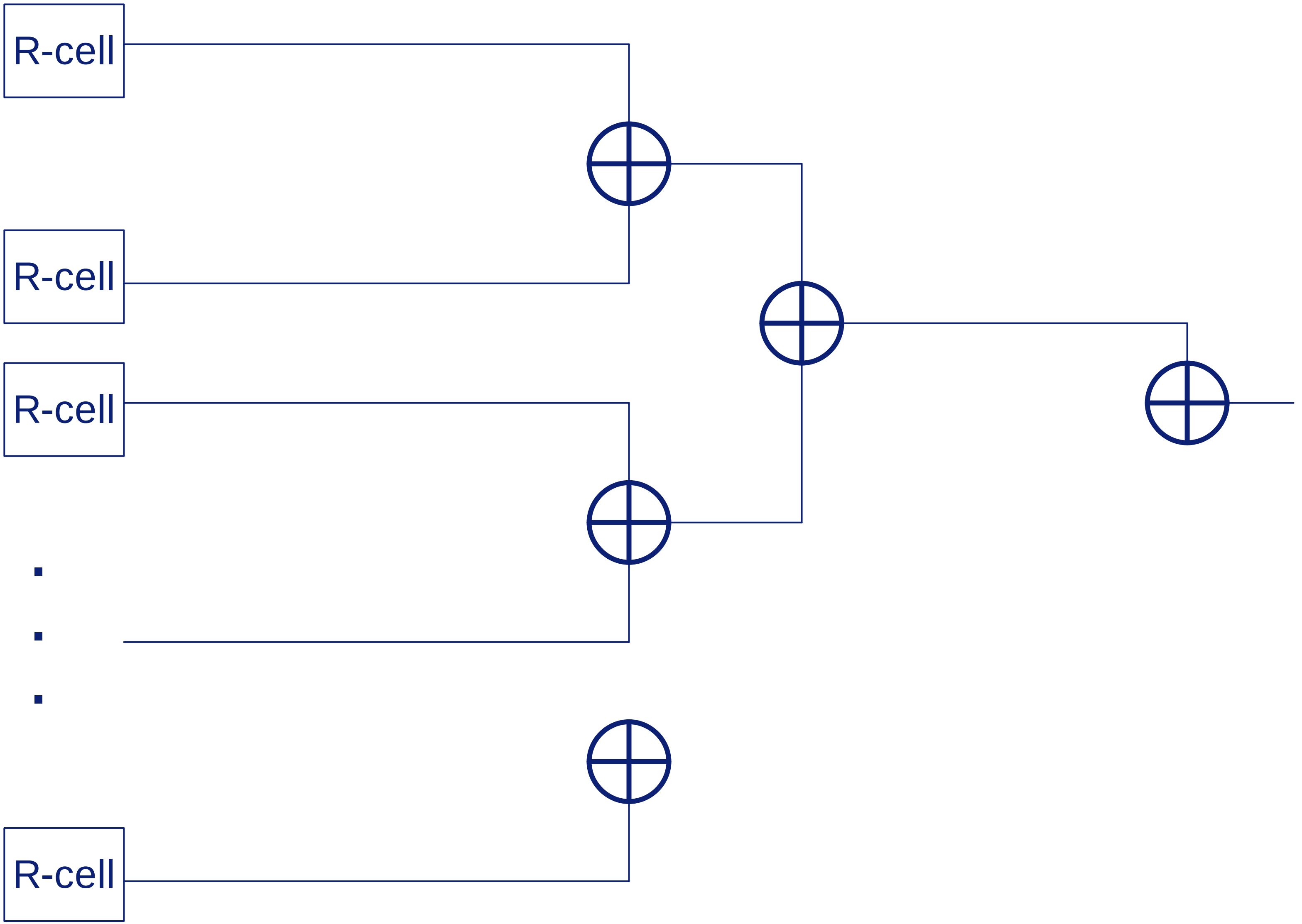
Sources of Randomness

- Ungoverned oscillators have random issues
  - Startup time
    - Low gain is helpful
  - Jitter

❖Note: Asymmetric delays reject external “locking” attacks

- Bi-stable (resolver) has random issues
  - Meta-stable balance point
  - Meta-stable voltages

Prototype System, 15 cells, all different



The Piling Up Lemma (handling bias)

- How can we remove bias?
  - The piling up lemma [Matsui 93]; Combination many random outputs biased by b_i produces a random output biased by b
    - b is much smaller that any b_i even if the individual b_i are large and have same kind of bias

$$b = \left|\mathrm{Prob}(X = 1) - \tfrac{1}{2}\right| = \left|\mathrm{Prob}(X = 0) - \tfrac{1}{2}\right|$$

$$b = 2^{n-1}\prod_{i=1}^{n} b_i$$

Testing

- Use the 16 DieHard tests
  - Each test produces a “squeezed” normal result
    - A Pvalue in a range from 0 to 1.000000
    - Very unlikely to find values near the tails (near 0 or 1)
- Rate each Pvalue as
  - A “hard”, “near” failure or “good”
  - Allow very few hard failures and/or a small number of near failures
    - Retest marginal cases if needed
      - Sometimes a random result will appear non-random but not on a consistent basis

Results

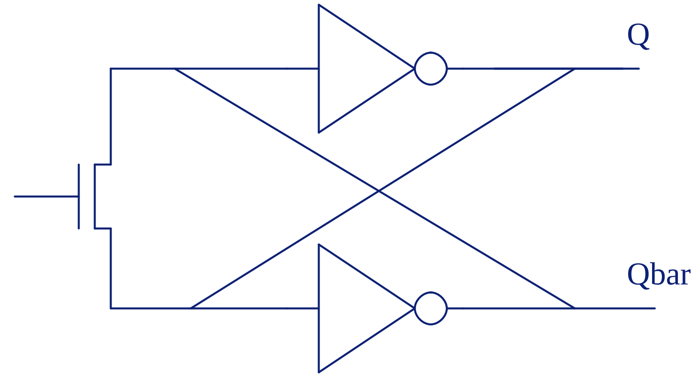
- Tested several designs
  - For each deign we tested 15-31 varieties and XOR of all varieties
  - Each design was replicated 8 times
- The best design (4-switch)
  - Is random for some varieties
    - At some voltages
  - Is random for XOR of 15 varieties over voltage range of 1.2 – 2.0 volts (1.8 is nominal)

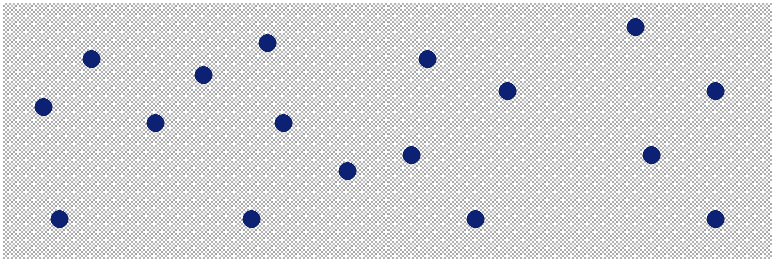
Detailed Results

- No special layout or custom circuits were used
  - Some identical cells passed and or failed
    - Suggests small layout changes have an affect
    - Each (XOR) copy requires 164 gates (very practical!!)
- At any voltage almost all of the varieties fail but the XOR always passes for all 8 copies
  - The results are random but biased
    - De-biasing always yields bits that pass

Thanks

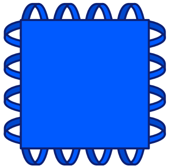
- Martin Rosner
  - circuit design
  - breadboard implementation
- Laszlo Hars, Hao Zheng
  - random theory
  - circuit design
- Raymond Krasinski
  - software support
- Philips Semiconductors





```
Main(argv,argc)
        {
        goto void;
        }
```

$



Conclusions

- Practical real random number generator can be built from standard digital circuits
  - Stable over voltage variations
- Work remains
  - Show good randomness over temperature change
    - Combination of voltage and temperature change
  - Verify physical source of randomness
    - Hopefully in the quantum mechanical sense
  - Verify resistance to electrical attacks

PHILIPS