A Hardware Random Number Generator

Stay Smart

Thomas Tkacik, Motorola

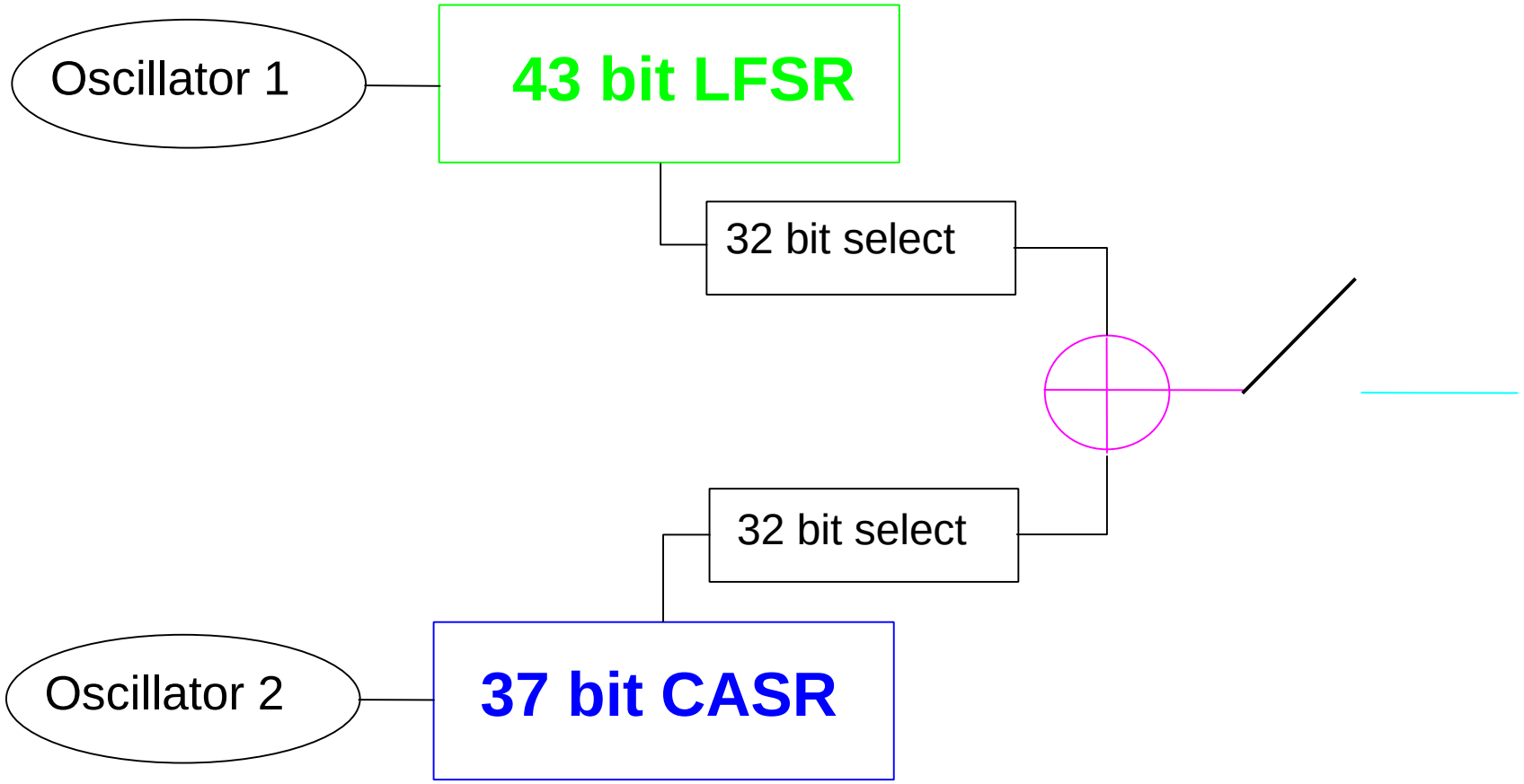
MOTOROLA

intelligence everywhere

Desired Properties of Random Numbers

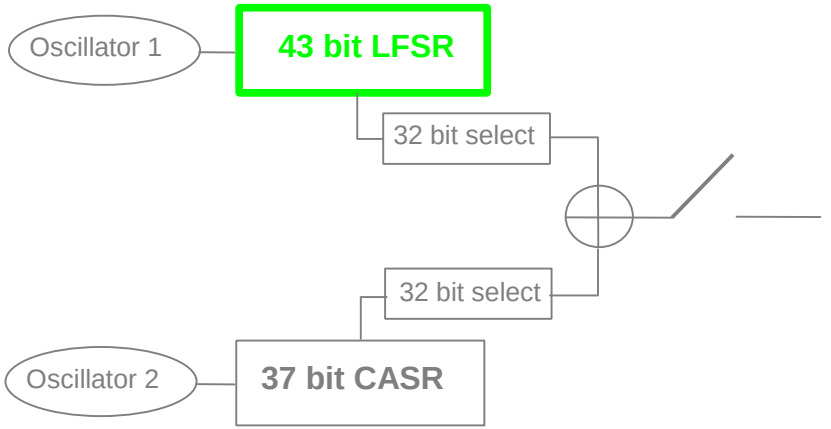
- Unpredictable
- Lack of bias
- Bit Independence
- Nonrepeatable
- Long cycle length

RNG Block Diagram



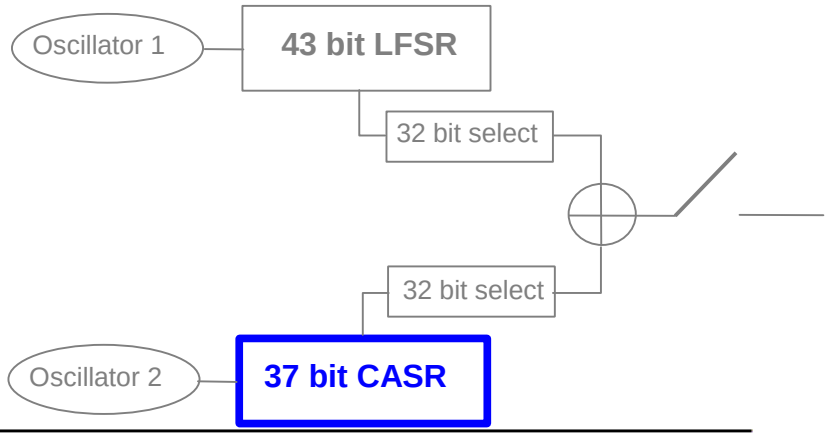
Linear Feedback Shift Register

- 43 bit LFSR
- Characteristic polynomial
  - $X^{43} + X^{41} + X^{20} + X + 1$
- Maximal length
  - *Cycle length* = $2^{43} - 1$
- There is a slight bias
  - *Bias* ~ 2^{-43}



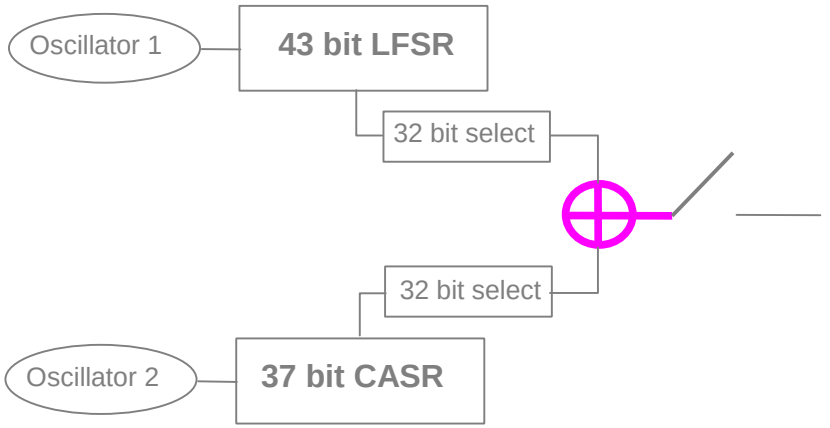
Cellular Automata Shift Register

- 37 bit CASR
- CA90 $a_i(t+1) = a_{i-1}(t) \wedge a_{i+1}(t)$
- CA150 $a_i(t+1) = a_{i-1}(t) \wedge a_i(t) \wedge a_{i+1}(t)$
- CA150 is at bit 28, CA90 used elsewhere
- Maximal length
  - *Cycle length = $2^{37} - 1$*
- There is a slight bias
  - *Bias ~ 2^{-37}*

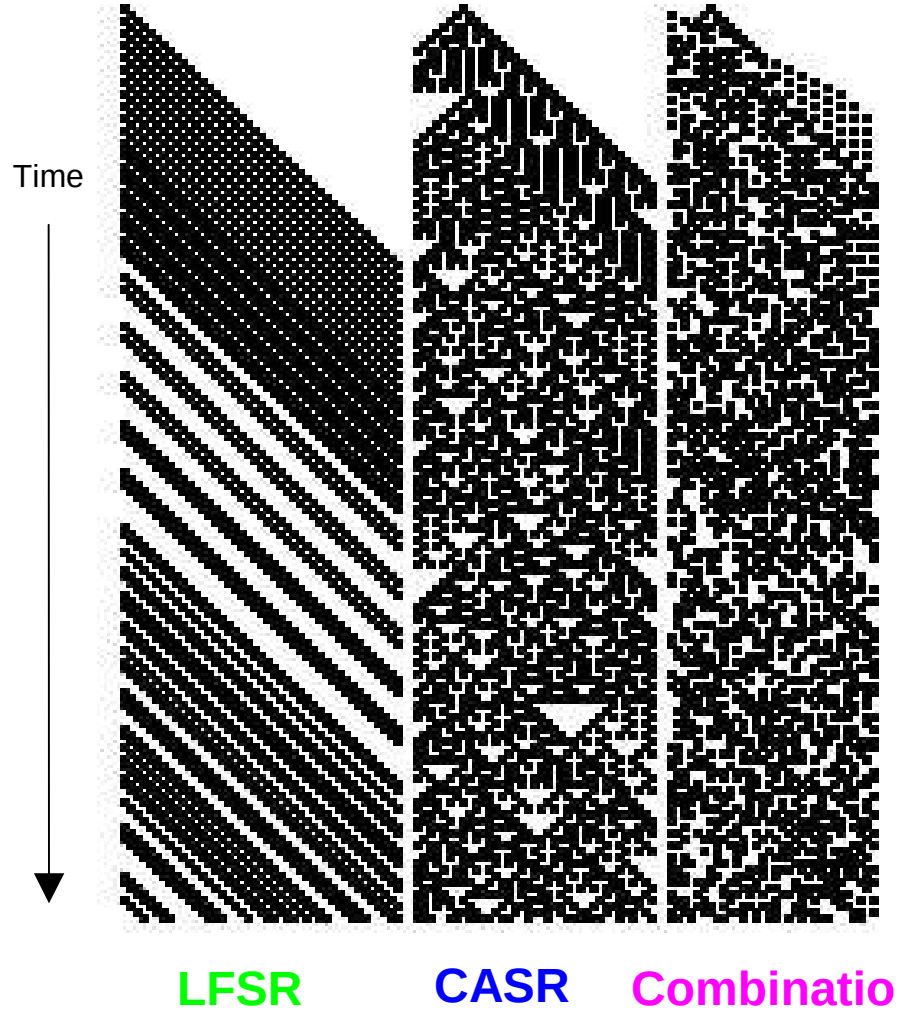


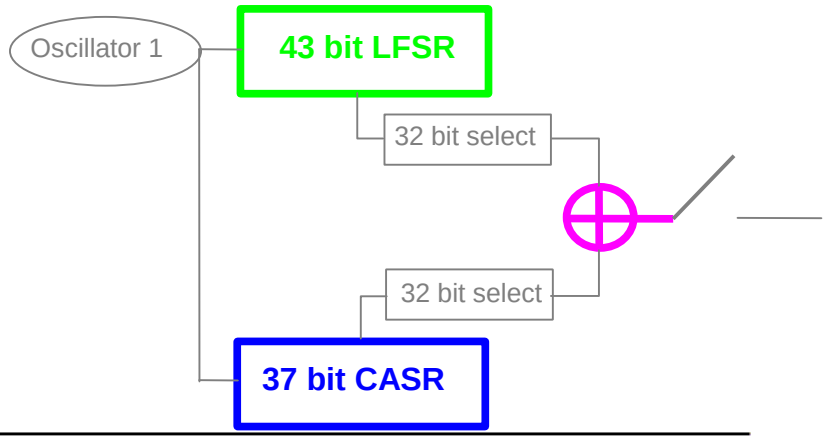
LFSR and CASR Combination

- Combination is formed by permuting and XORing 32 bits of LFSR and CASR
- The combination has a cycle length of
  - *Cycle length* = $2^{80} - 2^{43} - 2^{37} + 1$
- The bias is reduced to
  - *Bias* ~ 2^{-80}

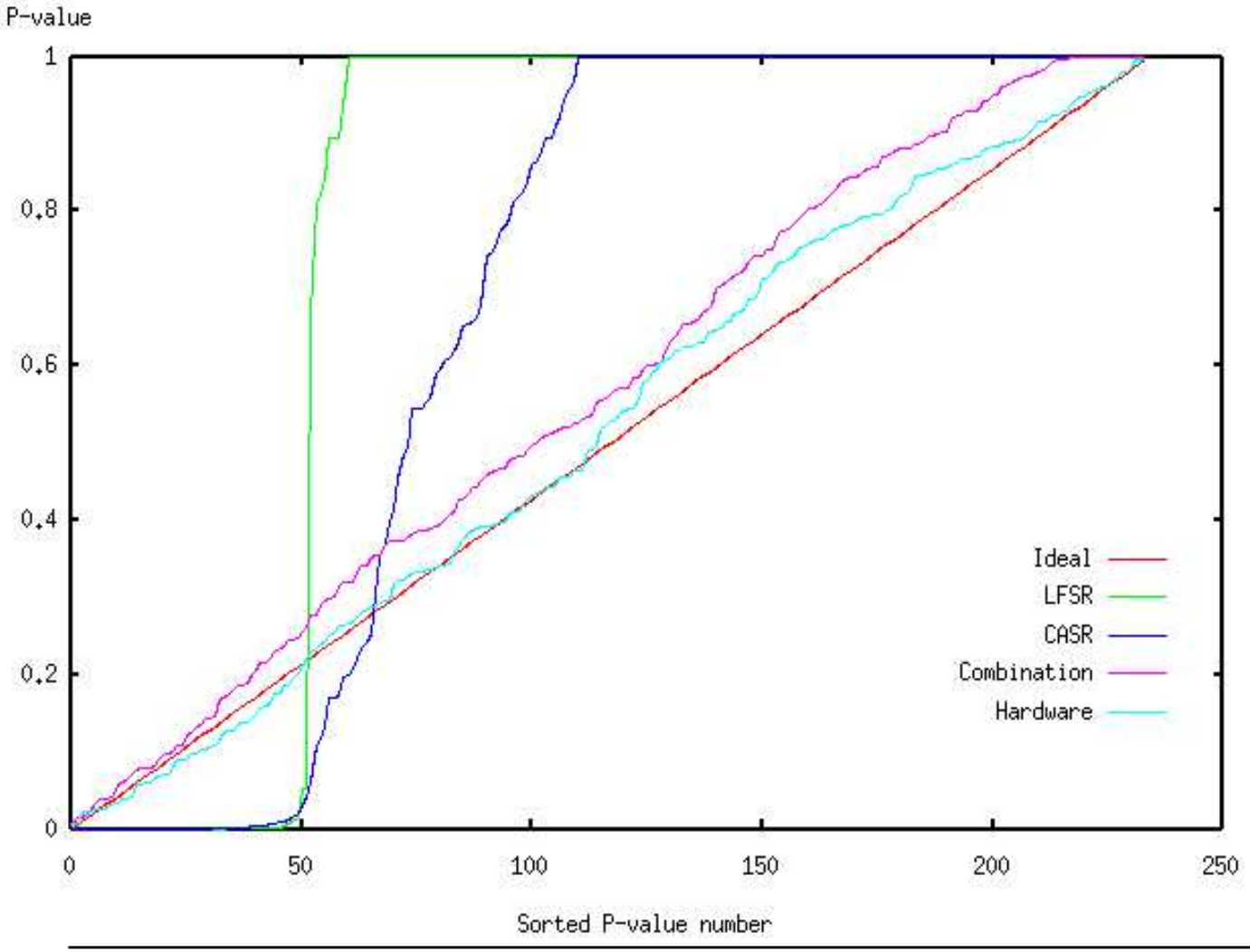


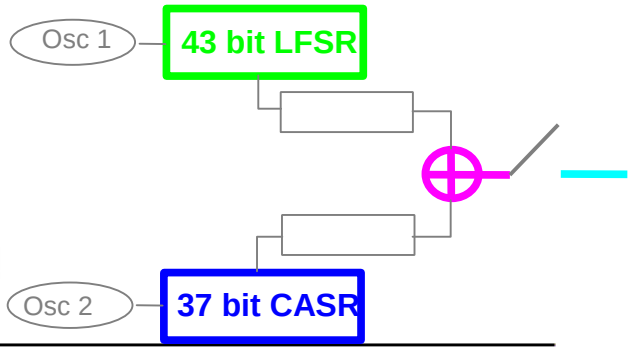
State-Time Diagram for LFSR, CASR and Combined Generator





DIEHARD Results for LFSR, CASR and Combined Generator





Summary

- A Hardware Random Number Generator composed of simple components
  - *43 bit LFSR*
  - *37 bit CASR*
  - *Oscillator's frequency's vary with voltage and temperature*
  - *State registers are not reset at power-up*
- Written as RTL
  - *The oscillators have instantiated inverters*
- The oscillator clocks can be turned off for low power applications