“The Collector”. Gigabit True Random Number Generator Using Image Sensor Noise

James Hughes, UCSC
Yash Gupta, UCSC

True Random Number Generators

- True random number generators have generally not scaled with Moore’s law.
- Noise in CMOS sensors has been widely studied in an effort to understand and reduce it without success.
- We embrace the CMOS sensor parallelism and intrinsic noise.

Entropy using Phonons

- Heat “particles”, in the form of vibrations jostle electrons from the valence band to the conduction band
- The number of disturbed electrons per unit time is a Poisson distribution
- Increases exponentially with temperature

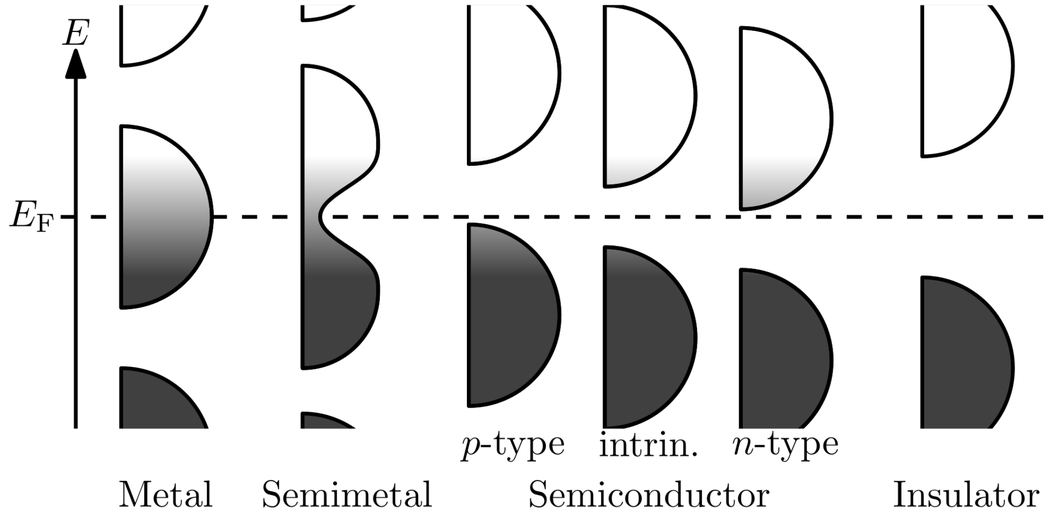
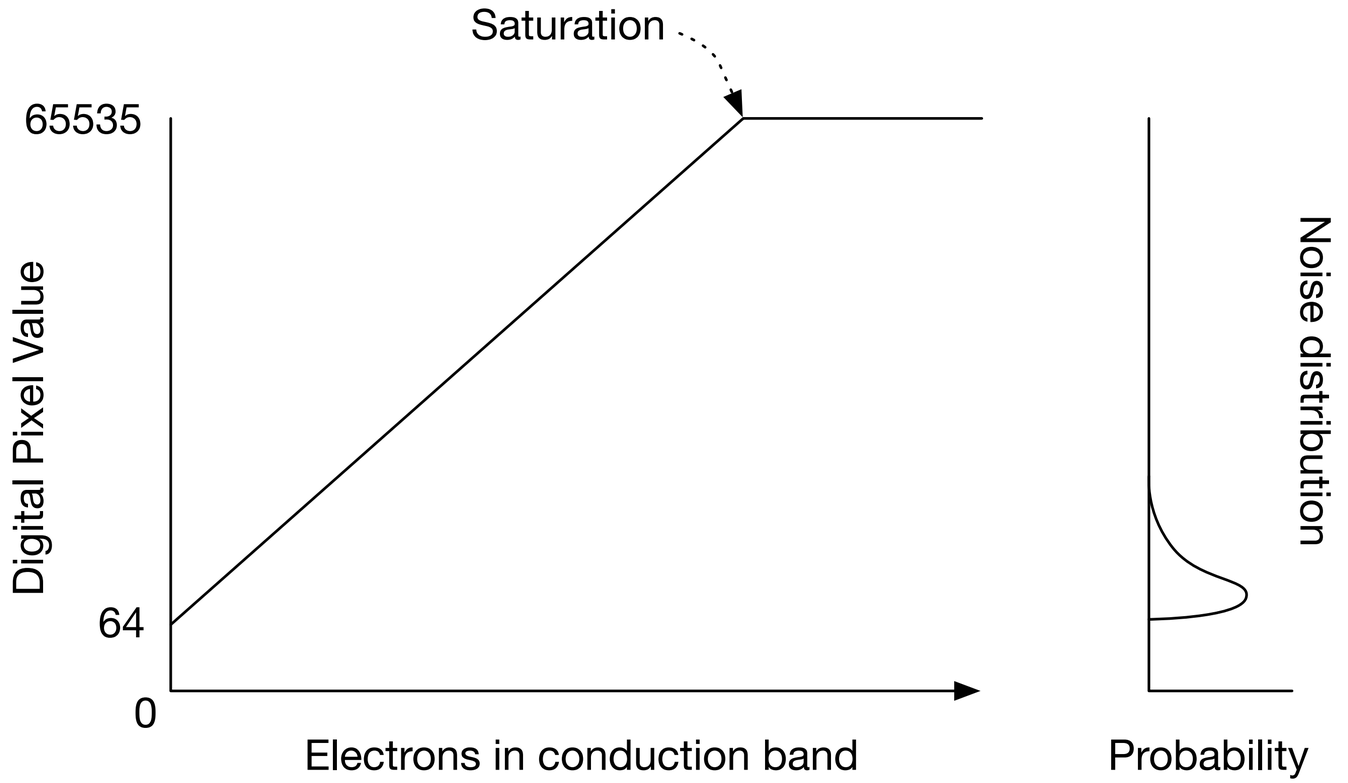


Figure 1: Bands of various materials [26]

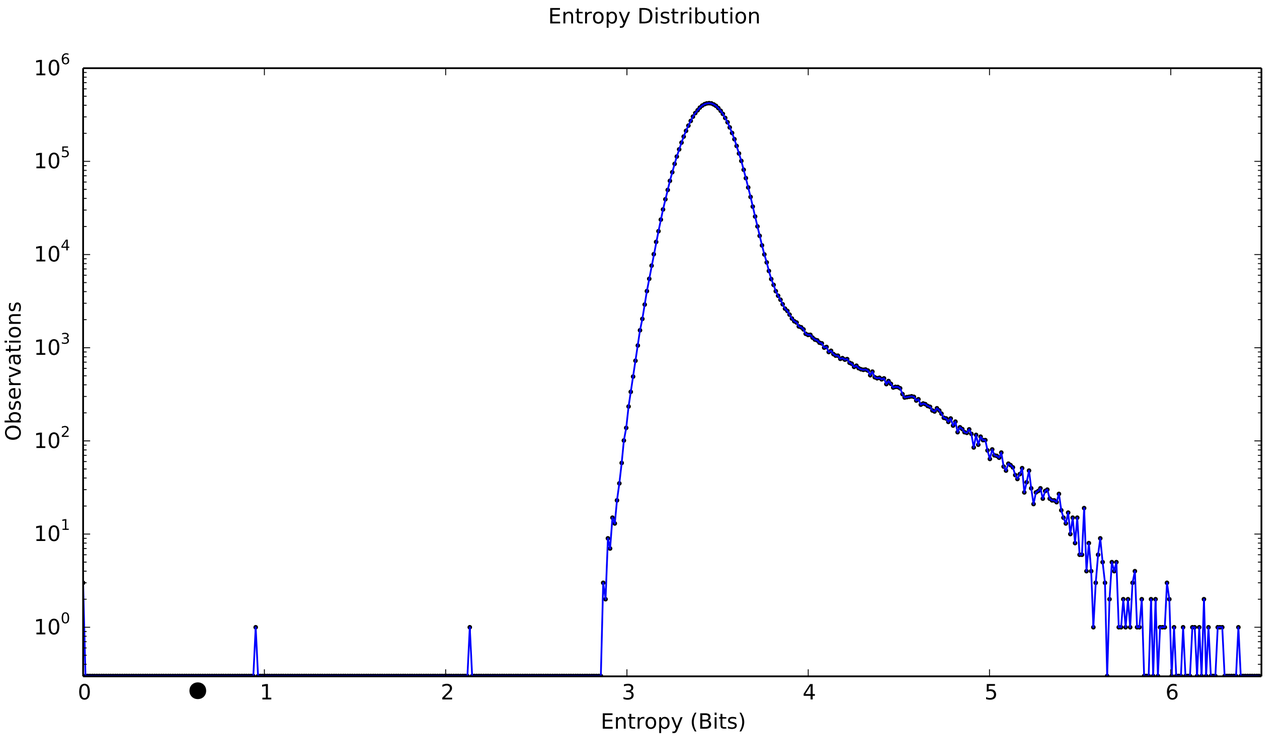
Adjustments to measure the noise

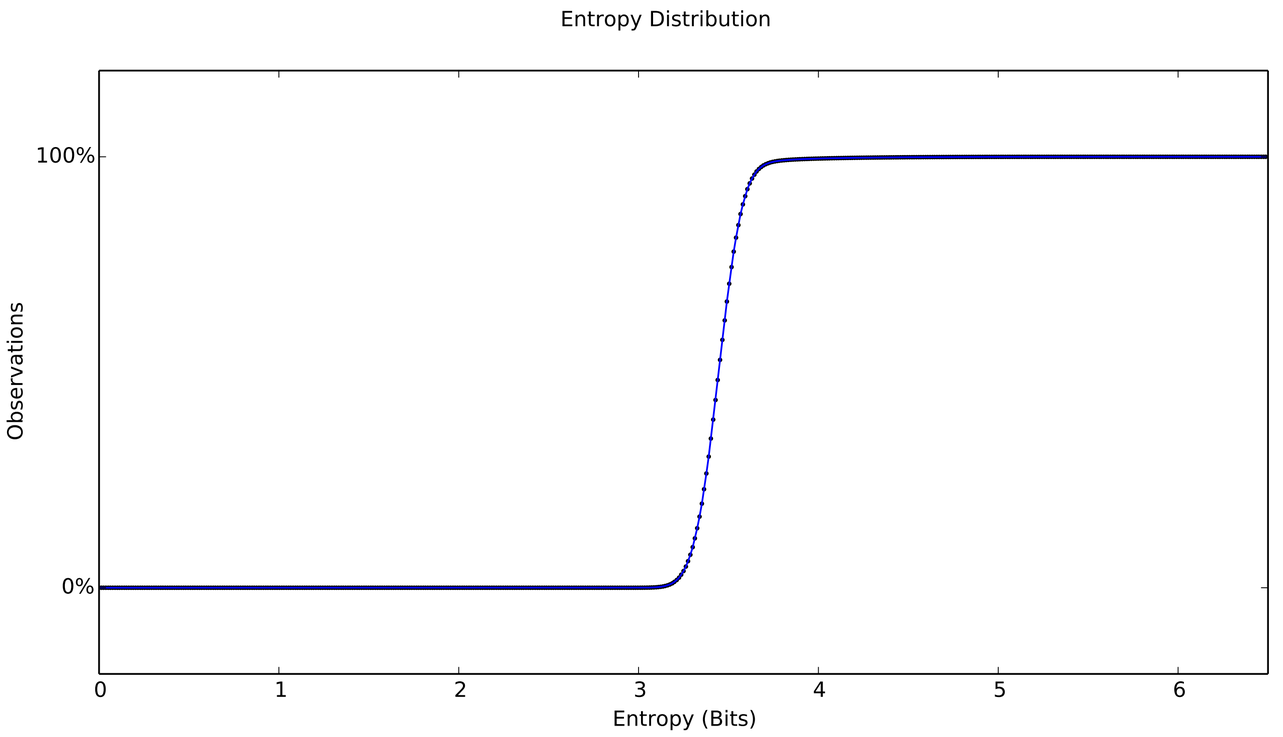
- Requires RAW



Measured Entropy

- Pixels individually measured over 100 pictures

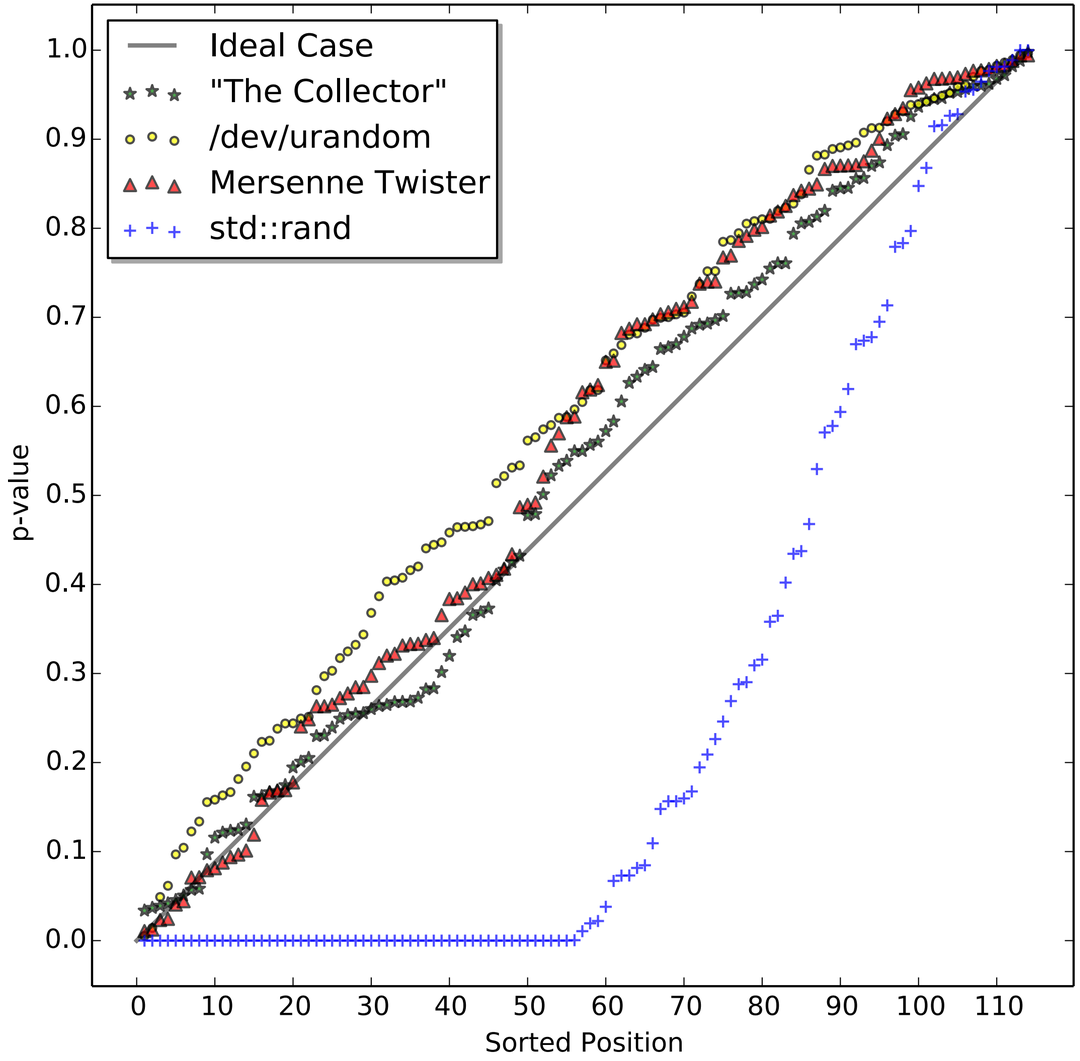




Whitening

- Eliminates the bias to be able to create usable random numbers
- Many methods
- Read the paper if you want one more

Results - DieHarder tests



Performance

- 3 bits of entropy per pixel
- 24Mp
- 30 Frames per second
- 2.16Gb/s

Go Slugs!