Investigating Integrated Single-Photon Optics for Power-Efficient Quantum Randomness

Ethan Gordon, Daniel Stanley

Here we look at an integrated system to utilize quantam randomness in linear optics. As outlined in Fig. 1, our system attenuates a laser down to single photons, sending them through a 50/50 beam splitter. Single-photon avalanche diodes (SPADs) at the end of each waveguide collapse the wavefunction, and which SPAD fires determines the output bit. Compared to classical pseudo-random schemes, we determined that this system is not power efficient for a practical number of bits, with power efficiency limited by the high break-down voltage and parasitic capacitance of the SPAD junction.

Photon Generation

The frequency of photon generation depends on the desired frequency of random bits (1GHz) and SPAD detection efficiency. To successfully generate a random bit, exactly one of the two SPADs must detect a photon. If more than one photon is generated, the probability of this happening depends on how the photons are split between the two SPADS and which are successfully detected. We find this probability to be $2(1-\frac{p}{2})^n - 2(1-p)^n$ for n photons and probability p of detection. If a laser produces a number of photons according to a Poisson distribution with mean λ, the probability of producing a bit becomes $2e^{-\lambda p}\left(e^{\frac{\lambda p}{2}}-1\right)$. To maximize this probability for a particular p we find $\lambda = \frac{2\log(2)}{p}$, and the probability of producing a bit is $\frac{1}{2}$ regardless of p. To produce random bits at a frequency f the photon detection cycle must run at $2f$. This informed the investigation of a SPAD quenching cycle that could complete in under 500ps.

System Design

Previous work [1] modeled the SPAD with a piecewise linear resistor approximating the non-linear region above the breakdown voltage and two parallel triggers allowing current to flow in the presence of a photon of self-sustaining current. We re-implemented this model (Fig. 2) using ideal switch elements, providing the behavior of a resistor in series with an ideal diode. We then tuned the I-V parameters to match an existing silicon SPAD model [2].

Model accuracy was verified using a simple passive quenching scheme and a shunt capacitance $C_L = 10pF$, where a single resistor at the cathode would act to drop the cathode voltage below break-down during the avalanche. Shown in Fig. 3, we verified the correct behavior: a near-instantaneous current draw followed by a quench time $\tau_q \approx R_{SPAD} * C_L \approx 445\Omega * 10pF = 4.5ns$.

For faster quenching and recovery times, we looked into a current-mirror approach [7]. In addition, this paper also gave us an estimate of the junction capacitance parameter, which, combined with the minimum detection area diameter of $8\mu m$ given by the process in [2], allowed us to estimate the parasitic capacitances at $5fF$. The final schematic, including a 500ps-clocked reset signal and photon signal, is shown in Fig. 4.

Power Analysis

Simulating the active quencher (Fig. 5), we were able to measure the power draw from both the low-voltage computation source and the high-voltage SPAD reverse bias source. The former was relatively small, averaging $8.88\mu W$ across two devices. However, due to the large voltages on the parasitic capacitances, the power draw through the SPAD was $592.1\mu W$.

To estimate the power required for the laser aparratus, we had to include timing inefficiencies each cycle due to photon detection $(30ps)$ and quenching circuit reset $(60ps)$. For a $1GHz$ goal, this means λ photons should arrive every $410ps$, for a laser photon frequency of $\lambda \cdot 2.44GHz$. With a known optical power per photon frequency [5], we find optical power as a function of SPAD detection efficiency. Finally, with a laser slope efficiency of $1.1\frac{nW}{\mu W}$ and threshold of $530nW$ [3], we can produce a graph of laser input power as a function of SPAD efficiency (Fig. 6). With a given SPAD efficiency of $\approx 50\%$, this figure is about $10\mu W$.

Comparison with Existing Pseudo-Random Solutions

One solution for producing pseudo-random bits at the hardware level is a Linear Feedback Shift Register. An LFSR consists of n Flip Flops in a shift register, the input of which is a function of bits in the register. With an optimal linear function producing input bits, an LFSR of n bits produces the same cycle of $2^n - 1$ psuedo-random bits over and over [6]. A larger register produces a longer cycle, and therefore more random-looking bits, at the cost of larger chip size and power consumption. A high level of randomness is essential for certain applications such as cryptography. Randomness test suites such as NIST are not a good measurement tool for this as the tests are pass-fail, and while LFSRs of more than 8 bits can fool most of the tests, even a 64-bit LFSR still fails at least one. Instead, used the LZMA compression ratio as a simpler estimate of bit entropy.

We used a pass-transistor design for our LFSRs to reduce power consumption [4]. We simulated LFSRs of different sizes at 1GHz and found a linear relationship between number of bits and power consumed. We now have a relationship between power and quality of randomness for LFSRs, and can compare to the power and true randomness of our quantum beam-splitter approach (Fig. 7). We find that the power needed for the beam splitter approach is comparable to a 93-bit LFSR, with the differences in randomness negligible for our metric.

Conclusion

With our current SPAD efficiency, it is not beneficial from a power standpoint to replace a LFSR pseudo-random number generator with a quantum beam splitter approach. The main source of power consumption was charging and discharging the parasitic capacitances around the SPAD. This could be mitigated by reducing these capacitances or reducing the high breakdown voltage of the SPAD.

References

[1] A. Dalla Mora, A. Tosi, S. Tisa, F. Zappa, "Single-Photon Avalanche Diode Model for Circuit Simulations," *IEEE Photonics Technology Letters*, Iss. 23, Dec, 2007.

[2] A. Gulinatti, I. Rech, P. Maccagnani, M. Ghioni, and S. Cova, "Large-area avalanche diodes for picosecond time-correlated photon counting," *Proceedings of ESSDERC*, Grenoble, France, 2005.

[3] A Maker, and A. Armani, "Nanowatt Threshold, Alumina Sensitized Neodymium Laser Integrated on Silicon," *Optics Express*, 21.22, 2013.

[4] Doshi N. A., Dhobale S. B., and Kakade S. R, "LFSR Counter Implementation in CMOS VLSI," *Intl. Journal of Comp., Electrical, Automation, Control Inf. Eng.*, vol.2, No:12, 2008.

[5] F. Hgo, G. Dario, S. Vincenz0, "An all-silicon single-photon source by unconventional photon blockade," *Scientific Reports*, Vol. 5, Jun. 2015.

[6] Peter Alfke, "Efficient Shift Registers, LFSR Counters, and Long PseudoRandom Sequence Generators," *Xilinx XAPP*, 052, July 1996.

[7] R. Mita, G. Palumbo, "High-Speed and Compact Quenching Circuit for Single-Photon Avalanche Diodes," *IEEE Transactions on Instr. Meas.*, VOL. 57, NO. 3, Mar. 2008.

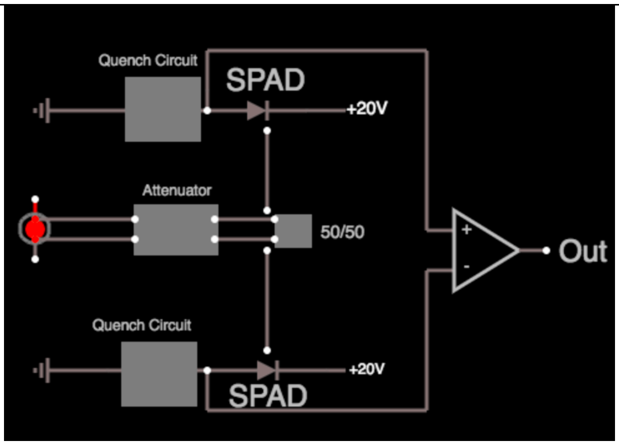

Fig. 1: High-Level Schematic of Proposed System

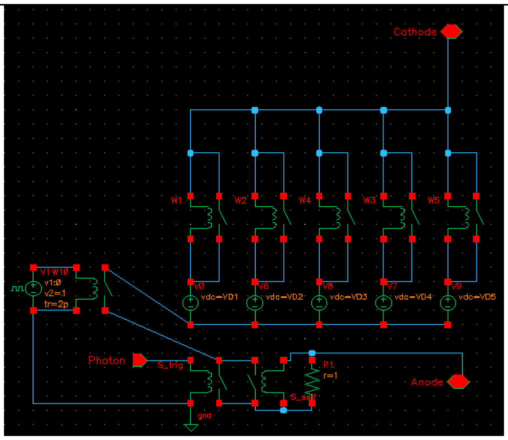

Fig. 2: SPAD Internal Schematic Without Parasitics

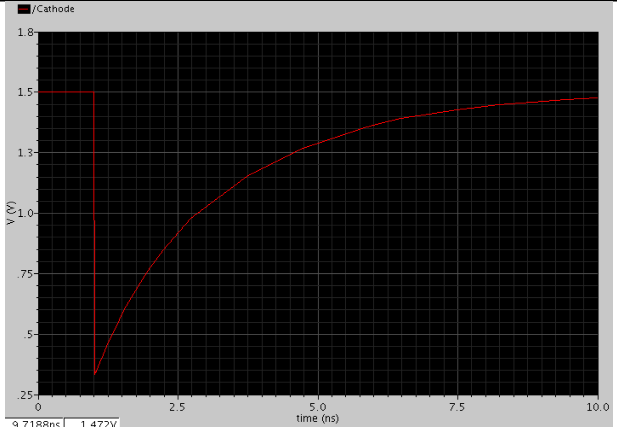

Fig. 3: Simulated Passive Quenching

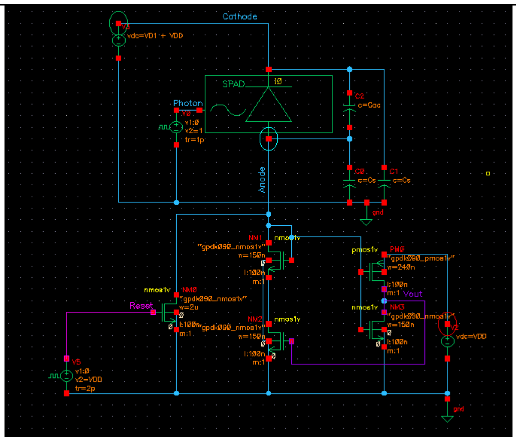

Fig. 4: Active Quenching Circuit Schematic

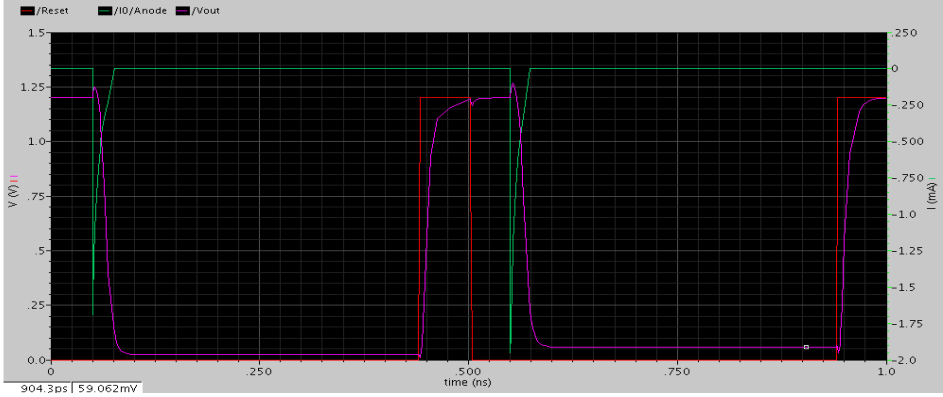

Fig. 5: Active Quenching Transient Simulation, including Reset Clock, output Voltage, and SPAD current draw.

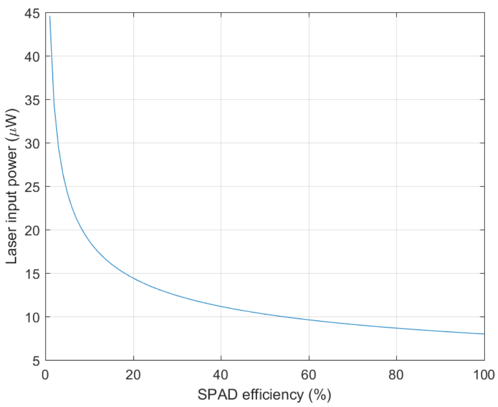

Fig. 6: Input Laser Electrical Power Required for 1GHz Operation

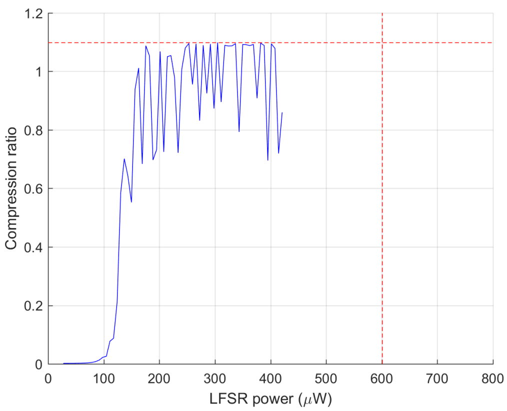

Fig. 7: LFSR Power vs. Entropy, with SPAD Power Consumption and Baseline Randomness Marked