Title: Power Efficient Pseudo-random Number Generators
Names: Felicia Guo, Jingyi Xu

Proposal:
Idea 2:
Pseudo random number generators are inherently limited by the period of random sequences. Currently proposed solutions to increased aperiodicity include using a physical randomness based RNG (such as one using oscillation based jitter [3]) to generate the seed for a PRNG [1], and using a potentially less random PRNG but introducing randomness from a Markov Chain based whitening scheme [4][5]. We plan to compare these two schemes, and evaluate the power consumption, area, and statistical randomness [2].

References:

[1]K. H. Tsoi, K. H. Leung and P. H. W. Leong, "Compact FPGA-based true and pseudo random number generators," *11th Annual IEEE Symposium on Field-Programmable Custom Computing Machines, 2003. FCCM 2003.*, Napa, CA, USA, 2003, pp. 51-61, doi: 10.1109/FPGA.2003.1227241.

[2] B. Elaine and K. John, "Recommendation for random number generation using deterministic random bit generators", *NIST SP 800–90 Rev A Tech. Rep.*, 2012

[3] Y. Zhang, J. Jiang, Q. Wang and N. Guan, "A Self-Timed Ring Based True Random Number Generator on FPGA," *2018 14th IEEE International Conference on Solid-State and Integrated Circuit Technology (ICSICT)*, Qingdao, China, 2018, pp. 1-3, doi: 10.1109/ICSICT.2018.8565658.

[4] V. R. Pamula, X. Sun, S. Kim, F. u. Rahman, B. Zhang and V. S. Sathe, "An All-Digital True-Random-Number Generator with Integrated De-correlation and Bias Correction at 3.2-to-86 MB/S, 2.58 PJ/Bit in 65-NM CMOS," *2018 IEEE Symposium on VLSI Circuits*, Honolulu, HI, USA, 2018, pp. 1-2, doi: 10.1109/VLSIC.2018.8502375.

[5]S. Callegari, R. Rovatti and G. Setti, "Embeddable ADC-based true random number generator for cryptographic applications exploiting nonlinear signal processing and chaos," in *IEEE Transactions on Signal Processing*, vol. 53, no. 2, pp. 793-805, Feb. 2005, doi: 10.1109/TSP.2004.839924.