Modeling SRAM cell stability for randomness evaluation of PUF cells

Yoav Weizman, Batya Karp, Osnat Keren
Bar Ilan University, Faculty of engineering

Physically unclonable function (PUF) circuit's implementations for cryptographic applications were studied extensively at the past decade. Among the numerous implementations proposed as PUF primitives, volatile SRAM based cells are considered as promising candidate for identification due to their simplicity and common conversion from standard libraries. The inherent metastable nature of the cross-coupled symmetric inverters is used as random bit generation where local process mismatches might bias each cell, into a unique stable state. The amount of mismatch eventually determines the stability of the cell in transitioning to a unique biased state during repetitive readings. There are several matrices which define the performance of any PUF implementation, reliability or stability is considered as one of the two key parameters, and for certain applications the most important parameter.

The common methodology to handle unreliable cells is by storing helper data and implementing error correction codes during the enrolment phase of the PUF [1][2]. Another approach (e.g. [3]–[5]) involve the detection and exclusion of unreliable cells. All together implementing these methods, could potentially lead to near 100% reliable array. However this implementation is achieved with the cost of custom cell design and considerable logic overhead. Thus assessment and management of cells reliability is having practical implications for SRAM PUF or TRNG implantations. Cross-coupled cells wake up value and evaluation of stability/uniqueness of this value were studied by [6], [7] based on measurements made on FPGAs and IC implementations of cells. An attempt to develop a model that describe the bitcell wakeup value was made by [8] using SNR analysis model.

In our study we propose a new model that relates between the mismatch parameters of the SRAM transistors to the probability of the cell to have a definite bias. The cell power-up process is modeled by simulations which include the various environmental and noise contributions to the cell settling into a consistent stable state. When standard SRAM array is powered up at realistic bias ramp rates, the dominant mechanism that determines the cross-coupled inverter latching is sub-threshold leakage. During the cell power-up electric charge start to leak through the two upper pMOS (see figure 1) , after some charge buildup at Q and Qb nodes this charge will also drain through the two bottom nMOS devices. Mismatch between the left and right sides of the circuit will eventually lead to latching when voltage difference between Q and Qb will become critical. In our model we correlate the threshold voltage mismatch and noise density to the probability for latching event of the cell. Assuming only sub-threshold leakage mechanism is relevant at the early stage before latching the KCL equation for the current flow (see figure 1) at the relevant junctions will be, assuming a quasi-stationary approximation: $I_{N1} \approx I_{P1} + I_{N2}$, $I_{N3} \approx I_{P2} + I_{N4}$ These equalities are perturbed by transistors shot noise which is the dominant noise mechanism for diffusion currents at the weak inversion regime. For very short integration times a saddle imbalance between the left equation and the right equation will yield deviation in charge buildup between the left and the right nodes of the coupled device which eventually induce latching. In order to validate the model we performed SPICE simulations with various threshold voltage mismatches between the coupled transistors in the cross-coupled inverter. The simulations were made in the presence of noise. The cumulative probability distribution of the repeated simulations was plotted Vs. various combinations of threshold voltage mismatches. The results are plotted in Figure 2 for several V_{th} combinations. The simulations show that the impact of pMOS mismatch is clearly the dominating parameter which determines the cell value. Nonetheless nMOS mismatch might compensate or enhance for the pMOS mismatch effect as shown in this figure. The combined effect of pMOS and nMOS mismatch will be weighted under the circuit current flow considerations and the model will consider the non-correlated probabilities of the 3 transistors that determine the two nodes mismatch. Another observation that will be demonstrated in this work is the impact of ramp-rate on the cell stability. This effect is shown in figure 3 where we can clearly observe the counter intuitive effect of ramp-rate over the cell stability. These phenomena will be explained in the light of our model.

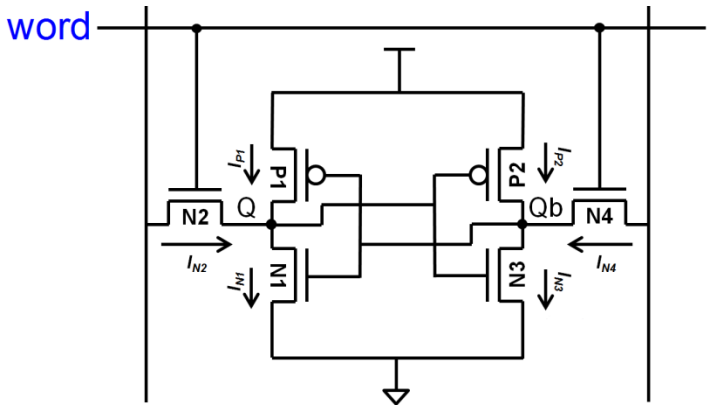

Figure 1 – SRAM cell

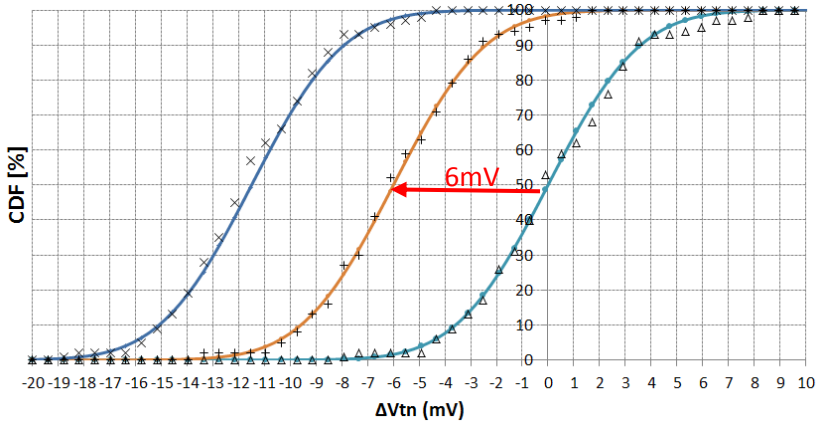

Figure 3 – CDF ΔVs. Vtn mismatch for different ΔVtp; (triangles) ΔVtp=0, (+) ΔVtp=1.5mV, (x) ΔVtp=3mV. We can observe the large shift of the CDF median (6 mV) when adding small ΔVtp

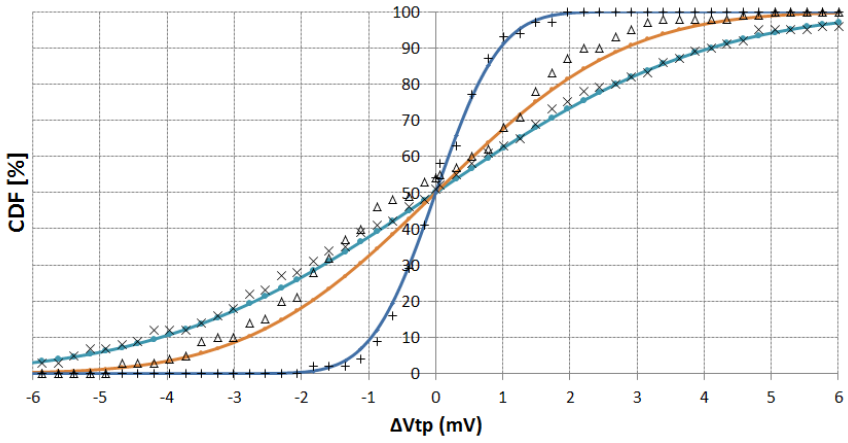

Figure 3 – CDF Vs. ΔVtp mismatch for different voltage ramp rates from 0 to 1.2V; (+) 0.1 usec, (triangles) 0.5 usec, and (x) 10 usec. The solid lines are normal distribution CDF fit with σ=0.75, 2.2 and 3.2 mV respectively

[1] Dodis, Y., Reyzin, L., & Smith, A. (2004, May). Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In International Conference on the Theory and Applications of Cryptographic Techniques (pp. 523-540). Springer Berlin Heidelberg.

[2] Maes, R., Tuyls, P., & Verbauwhede, I. (2009). Low-overhead implementation of a soft decision helper data algorithm for SRAM PUFs. In Cryptographic Hardware and Embedded Systems-CHES 2009 (pp. 332-347). Springer Berlin Heidelberg.

[3] Su, Y., Holleman, J., & Otis, B. P. (2008). A digital 1.6 pJ/bit chip identification circuit using process variations. IEEE Journal of Solid-State Circuits, 43(1), 69-77.

[4] Mathew, S. K., Satpathy, S. K., Anders, M. A., Kaul, H., Hsu, S. K., Agarwal, A., ... & De, V. (2014, February). 16.2 A 0.19 pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22nm CMOS. In 2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC) (pp. 278-279). IEEE.

[5] Hofer, M., & Boehm, C. (2010, August). An alternative to error correction for SRAM-like PUFs. In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 335-350). Springer Berlin Heidelberg.

[6] Maes, R., Tuyls, P., & Verbauwhede, I. (2008, November). Intrinsic PUFs from flip-flops on reconfigurable devices. In 3rd Benelux workshop on information and system security (WISSec 2008) (Vol. 17).

[7] Holcomb, D. E., Burleson, W. P., & Fu, K. (2009). Power-up SRAM state as an identifying fingerprint and source of true random numbers. IEEE Transactions on Computers, 58(9), 1198-1210.

[8] Cortez, M., Dargar, A., Hamdioui, S., & Schrijen, G. J. (2012, October). Modeling SRAM start-up behavior for Physical Unclonable Functions. In 2012 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT) (pp. 1-6). IEEE.