Design and Analysis of Feed-Forward PUF under Voltage Scaling in 32nm Technology

November 19, 2014

ECE658: Introduction to VLSI Design Principles
Partners: 1. Adithya Kommini
2. Ranjith Reddy Yallampalli
3. Vijay Keerthi Krishnamoorthy

Abstract

Physical Unclonable Functions (PUFs) are reliable functions which are completely based on physical characteristics unique to a chip. They implement challenge-response authentication. Beginning with basic PUFs implementation types, Arbiter PUF is one among them following a linear model for the delay paths. Linear model delay paths based PUFs are less-immune to model building attacks. Further addition of non-linear arbiters to the basic structure of Arbiter PUFs results in Feed-forward Arbiters exhibiting non-linear delay model. The induced non-linearity in delay models effect on the performance parameters of PUF i.e reliability, uniqueness is analyzed under different near-threshold and normal operating voltage conditions.

1 Motivation

The ever-increased usage of electronic devices coupled with unprecedented technological advancements is always plagued with the privacy issue related to cloning or the device being compromised altogether. It calls for a robust solution to provide strong privacy to the user and greater protection against the issue of duplication. PUFs seem to have provided a cost-effective solution in handling issues related to privacy/duplication. Most common methods of present day protection mechanisms are based on embodying cryptographic key in a non-volatile memory. Its digital form exposes it to easy attacks and needs a high cost inducing protection circuitry that needs to be powered on all the time. PUFs basically mirror the inter/intra chip random process variations. This property of PUFs enables the implementation of a low-cost device authentication process. The volatile nature of the PUF generated key makes it all the more difficult to mount attacks. Easy unique implementation techniques along with the feature

of extra-security based on the volatile nature of pattern key makes PUF an effective authentication solution.

2 Literature Review

Extensive research has been conducted on the role of Physical Uncolnable Functions in the field of device authentication based on unique secret key generation. One of the earliest work on PUFs belong to Lofstrom et al. (2000),which deals with identification of ICs by exploiting mismatch in silicon devices. Subsequently, the studies that followed Lofstroms work, identified how PUFs exploit the inherent variations in chip which in turn can be used to generate a unique pattern used for building a highly reliable authentication check mechanism. The major contributions of these works are demonstrating that the volatile nature of the pattern combined with the ease of implementation/ near-impossible prediction makes PUF a low-cost yet highly efficient substitute the traditional cryptographic based authentication mechanisms. PUFs are simple implementation structures that generate responses based on specific input challenge sequence combined with the inherent process variations associated with gates and interconnect. Several types of PUFs Arbiter PUF, Optical PUF, Coating PUF, Ring Oscillator PUF, Butterfly PUF, Glitch PUF and Mecca PUF have resulted from the extensive research (Maiti et al. (2013)) related to PUFs over the last one decade.

The figure below depicts the basic implementation idea of PUF showing the relation between a challenge and a response. At the evaluation and comparison stage, various parameters like uniqueness, reliability, randomness, steadiness and bit-aliasing are defined to compare the performances of two different PUFs on a common scale. Uniqueness is a measure of factor by which one chip can be distinguished from similar bunch of chips. Reliability on the other hand is a measure of how efficient the PUF is in reproducing the bits. Uniformity is a measure of how uniform the proportion of 0s and 1s in the response bits of the PUF.

Considering a basic PUF structure(Suh and Devadas (2007)), an arbiter PUF (Ruhrmair and Holcomb (2014))consists of delay circuit based on MUX instances and an Arbiter. The circuit consists of two identical delay paths (same layout length) and output Q is determined based on which path is faster. To evaluate the output of a particular input, both paths are enabled through a rising signal. The arbiter at the end toggles based on which path produces output faster.

One of the primary advantages of Arbiter PUF is the easy implementation, faster operation combined with less space being consumed on silicon when compared to other PUF structures like ring oscillator PUF. However, it does have a downside due to the easy implementation structure. It is prone to attacks based on model-building where the attacker can construct a precise timing model to learn the parameters based on different combination of inputs/outputs.

The Arbiter PUF is based on a linear timing model of the delay paths. A

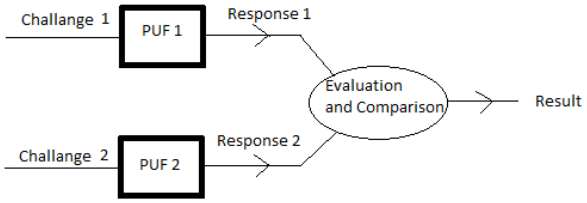

Figure 1: Basic idea of a PUF evaluation and comparison structure(Maiti et al. (2013))

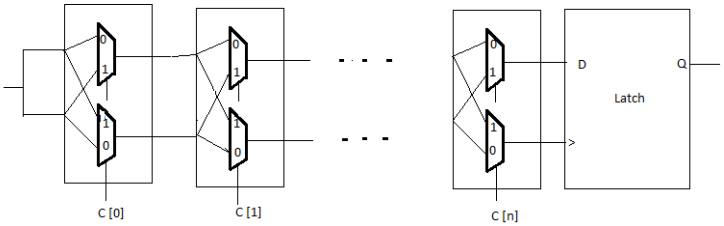

Figure 2: Basic structure of a Arbiter PUF where $C[i]$ is Challenge bits

modified version of PUF (Lim (2004)) with non-linear delay timing model for delay paths could offer more immunity to attacks. One such improved version of PUF implementation is the Feed-forward PUF.

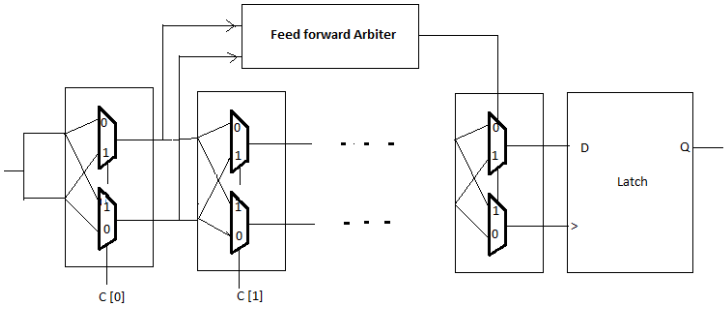

Figure 3: Basic structure of a Feed- forward PUF (Lim (2004))

The concept of Feed-forward PUF involves introducing internally generated (which can be hidden) challenge bits. These bits are no longer fed by the user. Instead the feed-forward signals provide the challenge bits (as determined by the race condition in that loop). The main advantage of a Feed-forward PUF is that it introduces non-linearity into the delay model by building a complex co-relation between internal signals using a feed-forward arbiter. This largely decreases prediction accuracy of the intermediate bits leading to increased immunity to adversary attacks.

2.1 Extension to Literature

The aim is to develop/introduce parametric variations which would increase the unpredictability of the circuit thus making the implementation more secure. The variation proposed in this work is to analyze and compare the performance parameters of Feed-forward PUF in different operating voltage regions (Nominal voltage, sub-threshold voltage). The exponential variation in Drain current with gate voltage at sub-threshold region results in significant variation in the arrival times of the signals through the delay path in the PUF circuit.

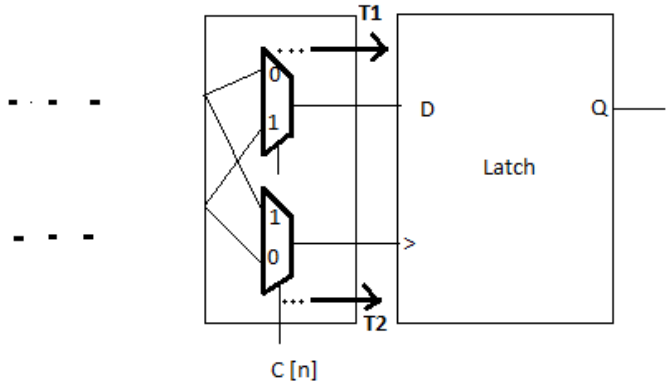

Figure 4: n-th challenge bit and Latch (Arbiter) of a PUF

Let arrival time of signal at D pin be : T1
Arrival time of signal at Clock ping be : T2
Slack time (window) between arriving signals of the PUF : T1˜ T2

The above figure shows the last stage of the PUF circuit with a latch (Arbiter) and pair of MUXes accepting n-th bit of the Challenge bits. A larger window indicating greater slack between arriving signals would in turn account for better performance parameters of the PUF. This variation could be analyzed further to correlate the change in the performance parameters. This may provide more

challenge and response pairs that can increase the unpredictability and can effectively counter the model attacks especially hybrid attacks. If time permits, the plan is to perform modeling attacks on the design and analyze the statistical metrics of the PUF circuit, especially its reliability.

3 Work Plan

Week 1[Nov 17 - Nov 23]	Designing the 64-stage feed-forward PUF [1,2,3] Hspice implementation of designed feed-forward PUF [1]
Week 2[Nov 24 - Nov 30]	Setting up of Monte-Carlo scripts [2,3] Monte-Carlo scripting for Nominal and Sub-Threshold voltage variations [1,2] Monte-Carlo scripting for variations in number of feed-forwards in PUF [3]
Week 3[Dec 01 - Dec 07]	Statistical analysis for Uniqueness[1] Statistical analysis for Reliability[2]
Week 3[Dec 07 - Dec 13]	Any improvements on the present design for better performance Report Generation [1,2,3]

References

Lim, D. (May 2004). *Extracting secret keys from integrated circuits*. Massachusetts Inst. Technology, Cambridge.

Lofstrom, K., Daasch, W., and Taylor, D. (2000). Ic identification circuit using device mismatch. In *Solid-State Circuits Conference, 2000. Digest of Technical Papers. ISSCC. 2000 IEEE International*, pages 372–373.

Maiti, A., Gunreddy, V., and Schaumont, P. (2013). A systematic method to evaluate and compare the performance of physical unclonable functions. In Athanas, P., Pnevmatikatos, D., and Sklavos, N., editors, *Embedded Systems Design with FPGAs*, pages 245–267. Springer New York.

Ruhrmair, U. and Holcomb, D. (2014). Pufs at a glance. In *Design, Automation and Test in Europe Conference and Exhibition (DATE), 2014*, pages 1–6.

Suh, G. and Devadas, S. (2007). Physical unclonable functions for device authentication and secret key generation. In *Design Automation Conference, 2007. DAC '07. 44th ACM/IEEE*, pages 9–14.