**Statistical Analysis of MUX-Based Physical Unclonable Functions**

**Abstract**

Physical unclonable functions (PUFs) can store secret keys in integrated circuits (ICs) by exploiting the uncontrollable randomness due to manufacturing process variations. These PUFs can be used for authentication of devices and for key generation in security applications. This paper presents a rigorous statistical analysis of various types of multiplexer-based (MUX-based) PUFs including the original MUX PUF, the feedforward MUX PUFs, the modified feed-forward MUX PUFs, and multiplexer-demultiplexer (MUX/DeMUX) PUF. The modified feed-forward MUX PUF structure is a new structure that is introduced in this paper. Three types of feed-forward PUFs are analyzed in this paper. These include feed-forward overlap, feed forward cascade and feed-forward separate. The performance analysis quantifies interchip and intrachip variations as a function of the number of stages, the process variation variance, the environmental noise variance, and the arbiter skew for different PUFs. Three other metrics of performance are also introduced and analyzed in this paper, which include reliability, uniqueness, and randomness. A PUF is more reliable if it has less intrachip variation. A PUF is more unique if the interchip variation is closer to 50%. A PUF is more random if its response bit is 0 or 1 with equal probability. Our statistical analysis shows that the intrachip variation is less dependent on the number of stages, N, if N is greater than ten. However, the interchip variation is dependent on N if N is less than 100. It is shown that the feedforward PUFs have higher intrachip variation than MUX PUFs; however, the modified feed-forward PUFs have significantly lower intrachip variation than the feed-forward PUFs. It is shown that the modified feed-forward cascade MUX PUF has the best uniqueness and randomness, while the original MUX PUF has the best reliability. The analysis presented in this paper can be used by the designer to choose an appropriate PUF based on the application’s requirement. This eliminates the need for fabrication and testing of many PUFs for selecting an appropriate PUF.

**Tools:**

* DSch
* Microwind