ABSTRACT

In this research, the properties of random numbers read from SRAM PUF have been investigated. The SRAM Memory cells readings was found to be identifiable, and they are classified into three types: quiet, noisy and neither quiet nor noisy bit. Two characteristics of random numbers are useful for cryptography key purposes. The noisy bit generated about 50% of '0' and '1', which can be used as a session key. The quiet bit generated close to 100% of all '0' and all '1', which can be used as an authentication tokens. Before using the noisy and quiet bit for application, the quiet bit was processed with fuzzy extractor, and the noisy bit was processed with randomness extractor. A statistic test program was used to analyze the random numbers. The context tree weighting was used to verify a truly random number by comparing the compressed file memory size to determine whether there is pattern in the noisy position. Moreover, minority percentage calculation and identify bit characteristic method were introduced and explained to identify noisy, quiet and neither of the bits. The probability calculation of random number was an algorithm that improved the speed and efficiency of identifying the attributes properties of the random numbers and helped estimate a position's identity without reading a position repeatedly a large amount of times.

Keywords - SRAM, random number generator, PUF