Tamper resistance evaluation of PUF in environmental variations

Submitted by grigby1 on Mon, 11/20/2017 - 12:27pm

Title
Tamper resistance evaluation of PUF in environmental variations

Publication Type
Conference Paper

Year of Publication
2016

Authors
Yoshikawa, M., Nozaki, Y.

Conference Name
2016 IEEE Electrical Design of Advanced Packaging and Systems (EDAPS)

ISBN Number
978-1-5090-6185-3

Keywords
arbiter PUF, composability, copy protection, counterfeit goods, counterfeit semiconductor components, Data models, delays, environmental variation, Immune system, machine learning attacks, machine-learning attacks, Mathematical model, physical unclonable function, Predictive models, pubcrawl, resilience, Resiliency, Resistance, semiconductor devices, Support vector machines, Tamper resistance

Abstract
The damage caused by counterfeits of semiconductors has become a serious problem. Recently, a physical unclonable function (PUF) has attracted attention as a technique to prevent counterfeiting. The present study investigates an arbiter PUF, which is a typical PUF. The vulnerability of a PUF against machine-learning attacks has been revealed. It has also been indicated that the output of a PUF is inverted from its normal output owing to the difference in environmental variations, such as the changes in power supply voltage and temperature. The resistance of a PUF against machine-learning attacks due to the difference in environmental variation has seldom been evaluated. The present study evaluated the resistance of an arbiter PUF against machine-learning attacks due to the difference in environmental variation. By performing an evaluation experiment using a simulation, the present study revealed that the resistance of an arbiter PUF against machine-learning attacks due to environmental variation was slightly improved. However, the present study also successfully predicted more than 95% of the outputs by increasing the number of learning cycles. Therefore, an arbiter PUF was revealed to be vulnerable to machine-learning attacks even after environmental variation.

URL