Low-cost fortification of arbiter PUF against modeling attack

Zalivaka S. S. (Foreign)[1],

Ivaniuk A. A.[2],

Chang C. H. (Foreign)[3]

2017 г.

1, 3 Foreign

2 Comp. Sci. Dept. Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus

Keywords: Authentication, Hardware, Field programmable gate arrays, Reliability.

INSPEC: Controlled Indexing: Authorisation, design for testability, field programmable gate arrays, Internet of Things, support vector machines.

INSPEC: Non-Controlled Indexing: Internet of Things, arbiter physical unclonable function, low-cost fortification, lightweight device authentication, robust device authentication, modeling attack resistance, machine learning attacks, multiple input signature register, MISR augmented 128-stage arbiter PUF, support vector machine, gradient boosting learning, design-for-testability, built-in logic block observer, Xilinx ZC706 FPGA chip.

Abstract: **A**rbiter Physical unclonable function (A-PUF) with exponential number of challenges is an ideal candidate to realize lightweight and robust device authentication in Internet of Things applications. Unfortunately, it is particularly difficult to attain highly reliable responses and increase its modeling attack resistance simultaneously. This paper presents an approach to reduce the vulnerability of A-PUF to machine learning attacks without compromising its high reliability and uniqueness. It utilizes a multiple input signature register (MISR) to process the input challenges. Our experiment results show that the accuracy of predicting the responses of a MISR augmented 128-stage arbiter PUF in FPGA implementation by support vector machine and gradient boosting learning algorithms with a training set of 100,000 challenge-response pairs has reduced drastically from 98% to 50%. If design-for-testability is mandatory, the MISR can be reconfigured from an existing built-in logic block observer, making this approach virtually free. Otherwise, the MISR carries a negligible hardware overhead of only 0.4% of the total available resources in an Xilinx ZC706 FPGA chip.

Published in: Proc. of IEEE International Symposium on Circuits & Systems (ISCAS 2017), Baltimore, MD, USA, 28-31 May, 2017. – P. 1600–1603. – DOI: 10.1109/ISCAS.2017.8050671

Internet link:

http://ieeexplore.ieee.org/document/8050671/