Reliable and Modeling Attack Resistant Authentication of Arbiter PUF in FPGA Implementation With Trinary Quadruple Response

Siarhei S. Zalivaka (Foreign)[1],

Alexander A. Ivaniuk[2],

Chip-Hong Chang (Foreign)[3]

2019

1 Foreign (School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore)

2 Faculty of Computer Systems and Networks, Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus

3 Foreign (School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore)

Keywords: Arbiter PUF, reliability enhancement, machine learning attack resistance, authentication protocol.

Abstract. Field programmable gate array (FPGA) is a potential hotbed for malicious and counterfeit hardware infiltration. Arbiter-based physical unclonable function (A-PUF) has been widely regarded as a suitable lightweight security primitive for FPGA bitstream encryption and device authentication. Unfortunately, the metastability of flip-flop gives rise to poor A-PUF reliability in FPGA implementation. Its linear additive path delays are also vulnerable to modeling attacks. Most reliability enhancement techniques tend to increase the response predictability and ease machine learning attacks. This paper presents a robust device authentication method based on the FPGA implementation of a reliability enhanced A-PUF with trinary digit (trit) quadruple responses. A two flip-flop arbiter is used to produce a trit for metastability detection. By considering the ordered responses to all four combinations of first and last challenge bits, each quadruple response can be compressed into a quadbit that represents one of the five classes of trit quadruple response with greater reproducibility. This challenge-response quadruple classification not only greatly reduces the burden of error correction at the device but also enables a precise A-PUF model to be built at the server without having to store the complete challenge-response pair (CRP) set for authentication. Besides, the real challenge to the A-PUF is generated internally by a lossy, nonlinear, and irreversible maximum length signature generator at both the server and device sides to prevent the naked CRP from being machine learned by the attacker. The A-PUF with short repetition code of length five has been tested to achieve a reliability of 1.0 over the full operating temperature range of the target FPGA board with lower hardware resource utilization than other modeling attack resilient strong PUFs. The proposed authentication protocol has also been experimentally evaluated to be practically secure against various machine learning attacks including evolutionary strategy covariance matrix adaptation.

Published in: IEEE Transactions on Information Forensics and Security. – 2019. – № 4 (14). – P. 1109 – 1123. – **DOI:** 10.1109/TIFS.2018.2870835.

Impact factor – 5.824.

Internet link to the article:

https://ieeexplore.ieee.org/document/8466897.