FPGA Implementation of Modeling Attack Resistant Arbiter PUF with Enhanced Reliability

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: Physical Unclonable Function, Arbiter PUF, enhanced reliability, modeling attack.

INSPEC: Controlled Indexing: Asynchronous circuits, copy protection, cryptography, field programmable gate arrays, integrated circuit modelling, integrated circuit reliability, learning (artificial intelligence), network routing.

INSPEC: Non-Controlled Indexing: FPGA, physical unclonable function, modeling attack resistant arbiter PUF, core lightweight hardware-intrinsic cryptographic primitive, device identification, edge computing, Internet of Things, IoT, routing constraint, machine learning attacks, cascaded switch mode delay representation model, security A-PUF.

Author Keywords: Physical Unclonable Function, Arbiter PUF, enhanced reliability, modeling attack

Abstract: Physical Unclonable Function (PUF) has now become a core lightweight hardware-intrinsic cryptographic primitive for device identification and authentication to secure edge computing in Internet of Things (IoT). The main challenge in most delay-based PUF implementations is the rival of response uniqueness and reliability. Due to routing constraint, implementation of delay-based strong PUF on FPGA tends to have either poorer reliability under varying operational conditions or vulnerably high predictability. Therefore, the design of high quality strong PUF often entails tradeoff between reliability and unpredictability (including uniqueness and randomness). Arbiter PUF is one of the most popular structures for FPGA implementation. It suffers from relatively low reliability and high susceptibility to machine learning attacks due to the linearity of its cascaded switch mode delay representation model. To overcome both problems simultaneously, we dichotomize the challenges to winnow out the unreliably weak challenges and obfuscate the remaining reliable strong challenges to increase its unpredictability against machine learning attacks. The security A-PUF is hardened at the expense of small hardware and latency overhead in preprocessing the challenges.

Published in: Invited Paper at Special Session on IoT Security: Protocol, Implementation and Attacks, in Proc. 18st IEEE International Symposium on Quality Electronic Design (ISQED 2017), Santa Clara, CA, USA, 13-15 Mar. 2017. – P. 313–318. – DOI: 10.1109/ISQED.2017.7918334

Internet link:

http://ieeexplore.ieee.org/document/7918334/