Presentation Submission to Cryptarchi 2017

TITLE OF THE PRESENTATION:

CLONE-RESITANT STRUCTURES IN MICROSEMI SOC UNITS

AUTORS: W. ADI, A. MARS, S. MULHEM

SPEAKER'S DETAILS:
Last name: Adi, First name: Wael, Email: w.adi@tu-bs.de
Job title: Professor, Organisation: Technical University of Braunschweig, EE Dept.
Postal address: Hans-Sommer Str 66, 38106 Braunschweig, Germany

key points of the presentation

1/ How to use unknown ciphers to crearte Unclonable physical units in FPGA technology
2/ Aging-resilient "Digital"- Physical Unclonable Functions (D-PUFs)
3/ Low-Cost clone-resistant modules in emerging non-volatile self-reconfiguring SoC units
4/ Clone-resistant entities for IoT environment

ABSTRACT OF THE PRESENTATION:

The concept of Secret Unknown Ciphers SUC is presented. SUC concept appears to be a strange one when proposing to use ciphers which nobody knows. The strongest practical secret is the one which nobody knows. Secret Unknown Ciphers SUCs were introduced by the author in 2009. SUCs are self-created, highly unpredictable unknown-ciphers accomodated in digital non-volatile self-reconfiguring VLSI units. Such VLSI units for accomodating SUCs are still not available. We postulate however, that such VLSI infrastructure may become available in the near future emmerging technologies. Realizing such ciphers is a challenging task requiring a "smart software GENNI" to create such ciphers within a short time and disappear out of SoC unit. A research group at the technical university of Braunschweig attained first promising basic results for efficient realization of such ciphers targetting Microsemi SmartFunsion FPGA SoC units or any similar technolog. The presentation demonstrates some basic generic protocols for using such SUC digital structures as clone-resistant modules. A broad spectrum of applications in consumer and vehicular electronics is expected when using such ciphers resulting with relatively low-cost, provable, clone-resistant or even possibly unclonable units. The technique allows manufacturer-independent personalization/security in SoC units having non-volatile technology.This allows, commercially-efficient, FPGA units, by creating tiny SUC module among the functional core structures to protect intellectual property rights in such units and create unclonable physical electronic units. The concept makes break-one break-all attacks infeasible on such systems. Each unit requires to be attacked individually and thus frustrates attackers by making legal units always cheaper than cloning them resulting with "pragmatic security". Few practical use cases and protype implementation samples are also presented.

KEYWORDS best describing the scope of your presentation (3 or 4):
- Clone-resistant or unclonable units
- Secret unknown ciphers SUCs
- Digital Physically Unclonable Functions (D-PUFs)
- Physical security and Identification in IoT Networks

Short bio of the speaker
Wael Adi, is a professor at the technical university of Braunschweig-Germany. He was Teaching and conducting research for more than 35 years in the field of computer engineering, error correction coding technology and security applications. He is holding a PhD and habilitation from the same university.