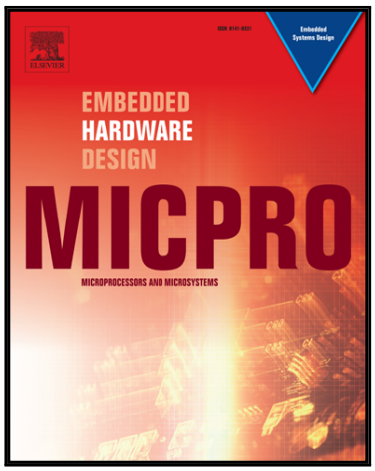

A Comparative Analysis of VLSI Trusted Virtual Sensors

Macarena C. Martínez-Rodríguez, Piedad Brox, Iluminada Baturone

PII: S0141-9331(18)30082-6
DOI: 10.1016/j.micpro.2018.05.016
Reference: MICPRO 2697

To appear in: *Microprocessors and Microsystems*

Received date: 19 February 2018
Accepted date: 25 May 2018

Please cite this article as: Macarena C. Martínez-Rodríguez, Piedad Brox, Iluminada Baturone, A Comparative Analysis of VLSI Trusted Virtual Sensors, *Microprocessors and Microsystems* (2018), doi: 10.1016/j.micpro.2018.05.016

Available online at www.sciencedirect.com

ScienceDirect

Microprocessors and Microsystems 00 (2018) 1–15

MICPRO

A Comparative Analysis of VLSI Trusted Virtual Sensors

Macarena C. Martínez-Rodríguez*, Piedad Brox, Iluminada Baturone

Instituto de Microelectrónica de Sevilla (IMSE-CNM), Universidad de Sevilla - Consejo Superior de Investigaciones Científicas (CSIC)
Américo Vespucio s/n. 41092 Seville (Spain)
Tel.: +34 95446666 - Fax: +34 95446600
*Corresponding author (e-mail: macarena@imse-cnm.csic.es)

Abstract

This paper analyzes three cryptographic modules suitable for digital designs of trusted virtual sensors into integrated circuits, using 90-nm CMOS technology. One of them, based on the keyed-hash message authentication code (HMAC) standard employing a PHOTON-80/20/16 lightweight hash function, ensures integrity and authentication of the virtual measurement. The other two, based on CAESAR (the Competition for Authenticated Encryption: Security, Applicability, and Robustness) third-round candidates AEGIS-128 and ASCON-128, ensure also confidentiality. The cryptographic key required is not stored in the sensor but recovered in a configuration operation mode from non-sensitive data stored in the non-volatile memory of the sensor and from the start-up values of the sensor SRAM acting as a Physical Unclonable Function (PUF), thus ensuring that the sensor is not counterfeit. The start-up values of the SRAM are also employed in the configuration operation mode to generate the seed of the nonces that make sensor outputs different and, hence, resistant to replay attacks. The configuration operation mode is slower if using CAESAR candidates because the cryptographic key and nonce have 128 bits instead of the 60 bits of the key and 32 bits of the nonce in HMAC. Configuration takes 416.8 microseconds working at 50 MHz using HMAC and 426.2 microseconds using CAESAR candidates. In the other side, the trusted sensing mode is much faster with CAESAR candidates with similar power consumption. Trusted sensing takes 212.62 microseconds at 50 MHz using HMAC, 0.72 microseconds using ASCON, and 0.42 microseconds using AEGIS. AEGIS allows the fastest trusted measurements at the cost of more silicon area, 4.4 times more area than HMAC and 5.4 times more than ASCON. ASCON allows fast measurements with the smallest area occupation. The module implementing ASCON occupies 0.026 mm^2 in a 90-nm CMOS technology.

Keywords: Virtual sensors, data security, hardware security, authenticated ciphers, piecewise linear approximation, CMOS integrated circuits.

1. Introduction

Virtual sensors estimate the value of a variable that is very difficult or costly to measure physically from others that can be measured easily with low-cost commercial sensors. The estimation usually makes use of models obtained with neural networks, fuzzy logic, or other types of approximation techniques such as piecewise affine (PWA) approaches. Among the latter, simplicial PWA (PWAS) functions were first employed for virtual sensors in [1] and, later, hyper-rectangular (PWAR) functions were used for their further simplicity in [2]. PWAR-based models partition the domain of the input variables (those easily measured) into hyper-rectangles and estimate the output (the virtual measurement) as an affine function whose parameters depend on the hyper-rectangle which the inputs belong to [3]. Figure 1 shows an example of a PWAR model that partitions a bi-dimensional input domain into 12 hyper-rectangles.