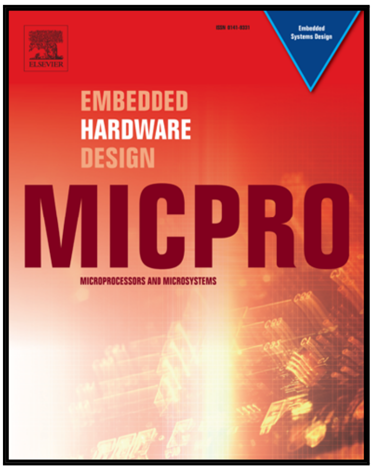

Efficient Security Zones Implementation through Hierarchical Group Key Management at NoC-Based MPSoCs

Johanna Sepulveda , Daniel Flórez , Vincent Immler ,
Guy Gogniat , Georg Sigl

PII: S0141-9331(17)30142-4
DOI: 10.1016/j.micpro.2017.03.002
Reference: MICPRO 2518

To appear in: *Microprocessors and Microsystems*

Received date: 16 June 2016
Revised date: 27 February 2017
Accepted date: 2 March 2017

Please cite this article as: Johanna Sepulveda , Daniel Flórez , Vincent Immler , Guy Gogniat , Georg Sigl , Efficient Security Zones Implementation through Hierarchical Group Key Management at NoC-Based MPSoCs, *Microprocessors and Microsystems* (2017), doi: 10.1016/j.micpro.2017.03.002

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Economics and Finance 00 (2012) 000–000

Procedia
Economics and Finance

www.elsevier.com/locate/procedia

Efficient Security Zones Implementation through Hierarchical Group Key Management at NoC-Based MPSoCs

Johanna Sepulveda[a]*, Daniel Flórez[b], Vincent Immler[c], Guy Gogniat[b], Georg Sigl[b,c]

[a]Institute for Security in Information Technology, Technical University of Munich, Germany
[b]Lab-STICC, South Brittany University, France
[c]Fraunhofer Research Institution for Applied and Integrated Security (AISEC), Germany

Abstract

Sensitive applications are split into the IP cores of the Multi-Processors System-on-Chip (MPSoCs). In order to isolate the sensitive communication among such IP cores, security zones based on conference keys agreement can be built. However, the flexibility and dynamic nature of MPSoCs force reshaping the security zones at runtime. It is still a challenge to achieve efficient computation and distribution of new conference keys in MPSoC environments. In order to solve this problem, in this work we propose the combination of two techniques: i) high performance NoC, able to efficiently communicate data and control packets in the system; and ii) hierarchical group-key management for efficient security zone modification. We implement three hierarchical protocols and we show that by decentralizing the security management of the rekeying process and using a two-level NoC, it is possible to achieve an improvement of the performance compared to the previous flat approaches.

Keywords: MPSoCs; Security; Group-key; NoC; high performance

* Corresponding author. Tel.: +49 (89) 289 – 28256.
E-mail address: johanna.sepulveda@tum.de