Application for Short Term Scientific Mission (STSM)

August 18, 2014

1 Project

ICT COST Action IC1204: Trustworthy Manufacturing and Utilization of Secure Devices

2 Involved Institutions

Home institution: Radboud University Nijmegen, The Netherlands, Lejla Batina, Kostas Papagiannopoulos

Host institution: Katholieke Universiteit Leuven, Belgium, Ingrid Verbauwhede

3 Visit Details

Visiting researcher: Kostas Papagiannopoulos – k.Papagiannopoulos@science.ru.nl

Visiting period: 20/09/2014 – 23/12/2014

4 Cost Estimation

Travel: 3*236/month=708 euros
Accommodation: 3*400/month = 1200 euros
Meals: 90*17/day = 1530 euros
Total: 3438 euros

5 Mission Statement

Nowadays, ubiquitous computing and the 'Internet of things' is gradually becoming a reality. A large, distributed infrastructure, consisting of numerous constrained devices,

has emerged and researchers have already identified a wide range of security and privacy risks stemming from it. To provide sufficient security in this setting, researchers have suggested lightweight ciphers that have a small footprint, reduced power consumption, sufficient speed and are protected from side-channel attacks.

My research interests are in the area of lightweight ciphers, efficient implementations and side-channels. So far, I have been investigating speed and size optimized cipher implementations with respect to software performance. For that purpose I have implemented several cipher designs (PRESENT, PRINCE, KATAN ciphers [1, 2, 3, 6, 5]) and supervised several cipher implementations. It is noteworthy that there exists a large number of trade-offs between different implementations. In addition, various objectives such as latency, area, throughput or side-channel resistance requirements led to various cipher designs, each one with its own distinct characteristics.

During the research visit, I intend to combine my existing, software-oriented knowledge of lightweight ciphers with the expertise of KU Leuven in hardware design. Specifically, the visit will be combined with a course on hardware-software co-design, such that I can establish a formal background on efficient design that maps software implementations to hardware circuits. I intend to apply the concepts of hardware-software co-design to produce efficient and flexible cryptographic implementations. Following this framework, I would like to investigate different implementation objectives for several lightweight ciphers and optimize their performance, especially the w.r.t. side-channel countermeasures and side-channel resistant designs [4].

Fast, efficient and low-cost ciphers can act as enablers for the 'Internet of things'. Establishing security and privacy in this context can enable and enhance a wide range of applications that rely on cryptographic primitives and assist transactions, commerce, entertainment and collaboration. Co-design can be very beneficial in this set by providing us with the flexibility and leading to the right implementation for the right purpose.

This project is aligned to COST working group 4 (reconfigurable devices for secure functions).

6 Plan Overview

- Attending the course on hardware-software codesign.
- Study and work towards efficient and flexible lightweight cryptographic implementations.
- Cipher implementations with side-channel resistance and countermeasures as the focal point.

References

[1] Andrey Bogdanov, Lars Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew Robshaw, Yannick Seurin, and Charlotte Vikkelsoe. PRESENT: An ultra-lightweight block cipher. In *Cryptographic Hardware and Embedded Systems – CHES 2007*, volume 4727 of *Lecture Notes in Computer Science*, pages 450–466. Springer, 2007. URL retrieved: 18-11-2013. `http://homes.esat.kuleuven.be/~abogdano/papers/present_ches07.pdf`.

[2] Julia Borghoff, Anne Canteaut, Tim Guneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Soren S. Thomsen, and Tolga Yalcin. PRINCE – a low-latency block cipher for pervasive computing applications. In *Advances in Cryptology – ASIACRYPT 2012*, Lecture Notes in Computer Science, pages 208–225, 2012. URL retrieved: 18-11-2013. `http://eprint.iacr.org/2012/529.pdf`.

[3] Christophe De Canniere, Orr Dunkelman, and Miroslav Knezevic. Katan and ktantan - a family of small and efficient hardware-oriented block ciphers. In *Cryptographic Hardware and Embedded Systems – CHES 2009*, volume 5747 of *Lecture Notes in Computer Science*, pages 272–288. Springer, 2009. URL retrieved: 18-11-2013. `http://www.cs.technion.ac.il/~orrd/KATAN/CHES2009.pdf`.

[4] Benoît Gérard, Vincent Grosso, María Naya-Plasencia, and François-Xavier Standaert. Block ciphers that are easier to mask: How far can we go? In *CHES*, pages 383–399, 2013.

[5] Kostas Papagiannopoulos. High throughput in slices: the case of PRESENT, PRINCE and KATAN64 ciphers. In *Radio Frequency Identification*, Lecture Notes in Computer Science, 2014. `http://rfidsec2014.cis.uab.edu/media/2014/07/12.pdf`.

[6] Kostas Papagiannopoulos and Aram Verstegen. Speed and size-optimized implementations of the PRESENT cipher for Tiny AVR devices. In *Radio Frequency Identification*, Lecture Notes in Computer Science, pages 161–175, 2013. `http://link.springer.com/chapter/10.1007/978-3-642-41332-2_11`.