SOUTH-EAST
EUROPEAN
RESEARCH
CENTRE

SEERC

SEERC
24 Proxenou Koromila Street
54622, Thessaloniki, Greece
Tel: +30 2310-253477/8
Fax: +30 2310 234205
www.seerc.org
Email: contact@seerc.org

OPEN SEMINAR SERIES

Wednesday 15 May 2019
09:30 – 10:30

Conference Room 8.2,
L. Sofou Building

"RESOURCE-EFFICIENT CRYPTOGRAPHY FOR UBIQUITOUS COMPUTING"

By
Dr Elif Bilge Kavun,
Department of Computer Science, TUoS

ABSTRACT

Compactness and mobility of very small-scale computing devices allow them to be deployed "pervasively" – such as in smart homes, logistics, e-commerce, and medical technology. Embedding these devices into everyday objects also indicates the realization of the foreseen "ubiquitous computing" concept. However, this in turn brought some concerns - especially, security and privacy.

For ubiquitous computing, the adversary model and the security level is not the same as in traditional applications due to limited resources in pervasive devices – area, power, and energy are actually harsh constraints for such devices. Unfortunately, the existing cryptographic solutions are generally quite heavy for these ubiquitous applications. In order to address the security problem of the resource-constrained devices, "lightweight cryptography" has been defined over a decade ago and many different lightweight cryptographic primitives have already been proposed. The published work so far mostly deals with hardware cost reduction. However, this is not the only important metric for such devices. Depending on the application, resource-constrained devices may need lightweight ciphers to be executed in one clock cycle, which still achieve a certain security level and a small footprint. Furthermore, as most of the pervasive computing applications are implemented in software on embedded microcontrollers, there is also a need for lightweight ciphers that result in efficient code size and execution time.

In our research, we understand lightweight cryptography also as "resource-efficient cryptography" and we aim to provide new "resource-efficient" solutions for resource-constrained devices, which address the mentioned gaps in lightweight cryptography. In the light of our investigations, we propose a low-latency and low-area lightweight block cipher PRINCE and a "software-oriented" lightweight block cipher PRIDE.

The seminar series is open to all members of *staff* and *students* of CITY and to any *externals* that wish to attend.

The University Of Sheffield.
International Faculty
CITY College.