

Lightweight Cryptography from an Engineer's Perspective

Dr. Axel Poschmann
Research Fellow
Division of Mathematical Sciences
School of Physical and Mathematical Sciences



Date : 6 March 2009 (Friday)
Time : 4.30pm – 5.30pm
Venue: SPMS-Executive Classroom 1, MAS-03-06
School of Physical and Mathematical Sciences

A widely shared view is that ubiquitous computing is the next paradigm in information technology. It fits that currently 98.8% of all manufactured microprocessors are employed in embedded applications and only 0.2% in traditional computers. The mass deployment of pervasive devices promises many benefits such as lower logistic costs, higher process granularity, optimized supply-chains, or location based services among others. On the other hand, many foreseen applications are security sensitive, such as wireless sensor networks for military, financial or automotive applications. Furthermore privacy issues will arise in many pervasive applications. An aggravating factor is that pervasive devices are usually not deployed in a controlled but rather in a hostile environment, i.e. an adversary has physical access to or control over the devices. This adds the whole field of physical attacks to the potential attack scenarios.

Pervasiveness implies mass deployment which in turn implies harsh cost constraints on the used technology. For ASICs (application specific integrated circuits) this means in particular that power, energy, and area requirements (in terms of Gate equivalents, GE) must be kept to a minimum. We will also show that Moore's Law will not relax these constraints but further increase the demand for lightweight solutions.

This talk gives an overview of lightweight cryptography. It covers lightweight block ciphers and lightweight hashing. We start with the design of DESL, a slightly modified lightweight variant of the Data Encryption Standard (DES). Then we look at PRESENT, which is the most compact block cipher for hardware implementations. Subsequently we use PRESENT as the basic building block for lightweight hash functions. Finally this talk is concluded and pointer for open research problems are provided.

Host: Coding and Cryptography Research Group, Division of Mathematical Sciences, School of Physical and Mathematical Sciences

SCHOOL OF PHYSICAL AND MATHEMATICAL SCIENCES

NANYANG TECHNOLOGICAL UNIVERSITY
SPMS-MAS-03-01, 21 NANYANG LINK, SINGAPORE 637371
FAX: +65 6515 8213 TEL: +65 6513 7423