

'IT Security for e-Health' Workshop: 4th Sept 2009

Microcontrollers, Elliptic Curves Cryptography

M. Mosdorf, W. Zabołotny, A. Grzanka, Institute of Electronic Systems, Warsaw University of Technology, Poland

The Challenge or problem

Research of the possibility of implementation of the Elliptic Curves Cryptography (ECC) algorithms on the microcontrollers with small computational power

Primary interests

Dissemination results of developed technology

The Approach to address the Challenges

In the personal medical equipment carried by the patient (recorders, portable monitoring equipment) reduction of the power consumption is essential. It allows to decrease the size of the rechargeable batteries and to extend the time between charging. Therefore, even though the prices and power consumption of advanced microcontrollers are continuously decreasing, it may be reasonable to use a simple microcontroller with minimal power consumption.

On the other hand, protection of the biomedical data (both their confidentiality and integrality) is an essential problem). Most advanced protection schemes use the asymmetric cryptographic algorithms to create the public key infrastructure (PKI).

Among different asymmetric cryptographic algorithms particularly important are the algorithms based on elliptic curves (ECC), because they are highly resistant to attacks at relatively small length of the key. Additionally they may be implemented with the moderate computation power. The above features lead us to begin research on possibility to implement the ECC algorithms on the processors with a small length of the word and small power consumption. Obtained results enable practical use of ECC algorithms in biomedical portable equipment.

Goals in attending workshop

Finding partners for pilot implementation, Common projects based on the presented results

For further information please contact:

a.grzanka@ise.pw.edu.pl