# Framework for Research of ECDSA

Tomáš Davidovič[1], Martin Novotný[1], Martin Havlan[2], Pavel Bezpalec[2]

[1]*CTU in Prague, FEE, Department of Computer Science and Engineering, Karlovo nám. 13, 121 35 Praha 2, Czech Republic*

[2]*CTU in Prague, FEE, Department of Telecommunication Engineering, Technická 2, 166 27 Praha 6, Czech Republic*

e-mail: davidt2@fel.cvut.cz, novotnym@fel.cvut.cz
e-mail: havlan@fel.cvut.cz, bezpalec@fel.cvut.cz

The paper describes a framework designed for evaluation of various approaches to ECDSA encryption. Our cryptographic core implementation uses an existing extensive communication framework provided by Combo6X cards.

Combo6X card has been developed within Liberouter project and it is used in wide range of networking applications. These include, but are not limited to, hardware routing, flow monitoring and fast network interfaces. To achieve this, the card contains two FPGA chips, it allows easy reconfiguration from the host PC and provides means for fast communication between applications and the FPGAs.

The goal of the framework is to provide easy way for comparing of normal and polynomial base approaches to ECDSA and also o compare affine and polar coordinates system performance. To achieve this we have implemented two versions of the framework. Both of them use micro-programmable controllers. The micro-programmable controller allows reconfiguration of the cryptographic core without actually flashing the chip itself.

First one has its arithmetic unit fixed and it uses micro-program only to choose between affine and polar coordinates. The second version is fully configurable in operation and allows changing both the coordinate system and the base for each input data. This enables evaluation of the cryptographic core that could easily communicate with devices using either standard; possibly even automatically swap the configuration based on the incoming data.

While the current implementation uses communication only via PCI, the interface is written in a highly universal manner and can be easily modified to interact with any device or component that can use a parallel, memory-like interface.

We will propose using of the core in network authentication, e.g. WiFi key exchange or digital signature technology used by routing information exchange. The reason is that for the same security, ECDSA requires fewer bits, and therefore also smaller encryption core and, consequently, it has lower power consumption. This is vital not only for current high-end cell phones and other portable wireless devices, but also for small SOHO routers and network access devices.

This work has been supported by CESNET, project 140R1/2005.