Name: Eng. Patrik Gallo

Finished degree: second, engineer

Final thesis: Authentication based on elliptic curves

Abstract: The Elliptic Curve Cryptosystem is an emerging alternative for traditional Public-Key Cryptosystem like RSA, DSA and DH. It provides the highest strength-per-bit of any cryptosystem known today with smaller key sizes resulting in faster computations, lower power consumption and memory. It also provides a methodology for obtaining high-speed, efficient and scalable implementation of protocols for authentication. This thesis provides an introduction to Elliptic Curves and how they are used to create a secure and powerful authentication system. It provides an overview of the Elliptic Curve Discrete Logarithm Problem. The authentication method is just based on the Discrete Logarithm Problem as well as on the verification of the hashes that are made from the unique message. The results of implementation are also discussed.

Name: Eng. Michaela Kreutzová

Finished degree: second, engineer

Final Thesis: Definition of Computer Language via User Interfaces

Abstract: Current software engineering practices result in creating software applications containing implicit knowledges about domain that is tangled with core functionality. This situation also reflects in the area of graphical user interfaces, for users the most important part of a program allowing interaction. This diploma thesis focuses on the problem of lack of research in the area of user interface language formalization and its efforts concentrate on outlining basic guidelines for creating user interface. It designs a software solution allowing definition of domain-specific languages via graphical user interfaces, recording and automation of user actions on application. The software solution is applied on a few examples of open-source Java applications.

Name: Eng. Mária Virčíková

Finished degree: second, engineer

Final thesis: Artificial Intelligence in Humanoid Systems

Abstract: This thesis deals with a usage of artificial intelligent techniques in humanoid robotics. The focus is on social robotics and how to use the interactive evolution for robotic dance system. In this diploma thesis the definition, principles and basic features of Interactive Evolutionary Computation are described and followed by an overview of their research and applications. This technique optimizes systems based on subjective human evaluation. The algorithm is applied to a system of the design of robotic dance, in which the evolutionary algorithm helps user to create choreography of the robotic dance. The system was implemented in language Python and simulation environment Webots. The experiments with several human subjects show that the interactive genetic algorithm approach to robotic dance choreography design aid system is promising.