Project description (158593/431)

Advanced Cryptographic Techniques (ACT)

*(*Financed by the Norwegian Research Council under the research program:
ICT-Security and Vulnerability)

SUMMARY

This project will focus on research in cryptology at an advanced international level. Project topics will be analysis and construction of symmetric and asymmetric cryptographic algorithms and protocols. In particular we will use our knowledge involving deep techniques from coding theory on cryptological problems where these techniques may improve upon the current state-of-the-art. The research will be carried out at the **Selmer Center** at the University of Bergen. The research group at the Selmer Center has been doing research in coding and cryptology for more than three decades and consists presently of 15 researchers, doctoral students, and frequent international visitors. The group aims to

- Complete 1 PhD theses in cryptology.
- Train a young post doc researcher that will also be an industry coordinator to ensure that knowledge of recent developments in cryptology will be transferred to Norwegian industry and to other Norwegian research groups.
- Publish regularly in leading international refereed journals and conferences.
- Organize one major national and one major international conference in cryptography.
- Organize courses in cryptography for Norwegian industry.

Introduction

In modern society, exchange and storage of information in an efficient, reliable and secure manner is of fundamental importance. There is an increasing amount of transactions using communications over the Internet and over mobile communication channels. Therefore secure communication will be essential for the exploitation of mobile communication and the Internet to its full potential, such as for the transfer of sensitive data in, for example, payment systems, e-commerce, m-commerce, health systems, oil and gas exploration monitoring, control system communications and in numerous other applications. For many of these applications, systems for authentication will also be necessary. **Cryptology** comprises the interrelated areas of *cryptography* and *cryptanalysis*. Cryptography is fundamental in order to protect information against wiretapping, unauthorized changes and other misuse of information. A cryptanalyst studies vulnerabilities of ciphers and other cryptographic techniques.

The coding/crypto group at the Department of Informatics at the University of Bergen, Norway has been working on reliable and secure communication problems using coding theory (for reliability) and cryptography (for security) for several decades in co-operation with many international research groups all over the world. The group is among the world's leading research groups in the integration of, and the interaction between, coding theory and cryptology.

In 2002, the Norwegian Research Council initiated an international evaluation of all ICT groups in Norway. The evaluation was performed by a selected group of international experts. The coding/crypto group received the best grade ***"Excellent"***, and the committee added that the group ***"may be the best ICT group of any kind in Norway and occupies a distinguished position in the international community",*** and that it ***"is one of the gems on the Norwegian Scientific scene, not just in the context of ICT"***.

Based on this evaluation, the University of Bergen decided to organise the coding/crypto group as a new research centre*,* ***Selmersenteret (The Selmer Center)*** named in honour of Ernst S. Selmer, a Norwegian pioneer in coding and cryptology who was previously a professor at the University of Bergen. This research centre will focus on research on reliable and secure communication.

Project description

Strong cryptographic algorithms, used in a correct manner, are essential in order to achieve any level of ICT security. The researchers at the Selmer Center have been working on the strength of cryptographic algorithms for many years. In recent years, it has become increasingly clear that coding theory and cryptology are related. To design good cryptosystems one may use elements from coding theory in many cases. For example, the new international block cipher standard AES is partly based on MDS codes, and some standard hash functions are constructed on the basis of special codes. Many approaches to cryptanalysis require deep insight into algorithms from coding theory.

The project will focus on the design and analysis of symmetric and asymmetric cryptography and cryptographic protocols, as well as on watermarking and fingerprinting, with a special emphasis on topics where we can draw on the Selmer Center's unique expertise in the border area between cryptography and coding theory. The research activities in the project will extend and complement those that already take place in the Selmer Center, funded by the University of Bergen, several NFR projects (mainly the Strategic University Program *Reliable and Secure Communications*), and EU projects. The topics may include, but are not confined to, those on the following list:

- *Analysis and design of secure, fast and practical encryption algorithms.*
- *Construction and analysis of block ciphers.*
- *Coordinate sequences and stream ciphers.*
- *Provably secure systems.*
- *The cryptanalysis of cipher primitives using message-passing algorithms.*
- *Design of hash functions in particular by using coding theory.*
- *Construction and analysis of message authentication codes (MACs).*
- *Design of authentication codes using coding theory.*
- *Analysis of stream ciphers using sequences and coding theory.*
- *Quantum coding and cryptology.*
- *Using error-correcting codes for digital fingerprinting, watermarking, and copyright protection.*
- *Network security and secure multi-party computation using codes on graphs.*
- *Security in wireless networks.*

Dr. Scient candidate and Post Doc researchers

The theoretical training of the doctoral students will consist of courses and seminars on an advanced level. These may be specialized courses and seminars focused on topics within cryptography, information security, and coding theory, but we will also draw on the courses on computer science at large, as taught in the Department of Informatics, or the courses offered at other departments within the University of Bergen.

Guest researchers

Guest researchers make up a valuable research resource, which we have previously used on several occasions with great benefits. These guests may be researchers on a senior level who are on sabbaticals or who for other reasons may be able to visit us for an extended period. In this situation the researchers will not receive ordinary salary from us, but instead a compensation for travel and extra living expenses.

Conference and workshop participation and organization

It is important to maintain a continuous contact with the leading edge of international research. The only way to achieve this is to participate actively in the research community. This can be achieved by several means. We are members of ECRYPT, a Network of Excellence in the European FP6 program. In order to increase our own visibility in the international community as well as the national awareness of cryptology, and also in order to do our share to promote cryptology internationally, we plan to organize at least one such conference or workshop during the project period. We will organize the WCC in Bergen in 2005 (Workshop on Coding and Cryptography; held in Paris in 1999, 2001, and 2003).

Courses in cryptography for industry

We have previously conducted courses on cryptology for Norwegian companies. We intend to do so also in the future.