Project description (146874/420)

# Reliable and Secure Communication (RASC)

*(*Financed by the Norwegian Research Council as a Strategic University Program)

**SUMMARY**
The project Reliable and Secure Communication (RASC) is a four-year Strategic University Program (SUP) in coding theory and cryptology, headed by Professor Tor Helleseth. The project runs during the period (2002-2005). The goal is to do strong and broad based research on a high international level in both coding theory and cryptology, with particular attention to the interaction between these two areas. We expect this focus to bring new and important scientific and applied knowledge to both fields, and we will publish the results in leading international journals. We will train younger researchers and will transfer results from recent research in these areas to Norwegian industry.

**The goals include**:

- Extend international research collaborations with other world leading research groups.
- Publish results in leading international refereed journals and conferences proceedings.
- 2 PhD's to be completed.
- Train one post.doc.
- Transfer results from recent research in coding theory and cryptology to Norwegian industry.

**A short description**
In recent year there has been a vast increase in the amount of data which is purchased, transmitted, compressed and stored every day, in particular via Internet. The need for efficient, reliable and secure communication is more important that ever before. Error correcting codes and cryptography are essential parts of the solutions to these problems for the society. This has created a crucial demand for highly qualified researchers working on secure and reliable digital communication. We will train young researchers and increase contact with industry to assist them to base solutions for secure and reliable communication on recent research in these areas.

In this project, we will do research in areas of error correcting codes and cryptography with emphasis on the interplay between these two areas. Some of the topics to be investigated are:

- Analysis and design of secure, fast and practical encryption algorithms.
- The theory of hash functions and authentication codes based on error correcting codes.
- Sequences with optimal correlation properties for CDMA applications.
- Efficient decoding algorithms.

**Description of the proposed scientific activity**
We will strengthen and broaden both the coding theory and cryptology activities, with a particular focus on the interplay between the two fields. In recent years, there has been an increasing interaction between coding theory and cryptology and we are convinced that such interaction will be increasingly important and give significant new knowledge in both areas.

**Cryptology**
It is the intention of the group to continue the analysis and design of secure, fast and practical encryption algorithms.

The hash function constructions of Knudsen and Preneel are still rather new, and the exact security of the proposals is still an open problem. Also, interesting extensions of the constructions using non-linear codes have yet to be fully explored. It is the intention of the group to analyze and further develop the theory of hash functions based on encryption algorithms and codes.

Traditionally, computationally secure message authentication codes, also known as MAC algorithms, have been based on block ciphers and/or hash functions. Seen in the light of recent developments in both block ciphers and hash functions, both of which tend to have bigger block sizes, there is a need to develop new methods for building MACs from these primitives. Also recently, improvements have been found in the area of information theoretically secure authentication codes, also called A-codes, both in terms of speed of computation and of the key size. The group has the expertise to contribute in these areas and intend to do so.

**Coding theory**
The main emphasis will be to continue and extend problems initiated during the last few years, along with other problem areas that will play an important role in the future.

- Design and analysis of sequences, e. g. for channel measurement, spread spectrum, code graph design, random number generation, or applications within cryptology,
- Codes over rings,
- Optimal codes and distance properties of classes of codes, including turbo and LDPC codes,
- Decoding algorithms and related problems,
  - Newton radius problems,
  - The structure of codes, including weight hierarchies and trellis structure,
  - Iterative decoding and codes on graphs,
- Codes for error detection.

In addition, we will open up research in some other areas that we believe will become increasingly important. Foremost among these new areas are coding for wireless communications.

**The interaction between coding theory and cryptology**
We will focus on coding theoretic problems related to areas that have a significant interaction with cryptology. Some relevant areas are

- Correlation of sequences,
- Hash function design,
- Decoding methods and their application to correlation attacks on stream ciphers,
- Weight hierarchies of codes,
- Error correcting codes used for watermarking and copyright protection,
- Quantum coding and cryptology,
- APN mappings,
- Authentication codes,
- Coding theoretic and cryptographic aspects of the security of wireless communication,
- Network security and secure multi-party computation using codes on graphs.