Building Public Key Crypto-Systems from Semi-Rings

Joachim Rosenthal
University of Zürich
Mathematics Institute
8057 Zürich, Switzerland

Cryptography has a long history and its main objective is the transmission of data between two parties in a way which guarantees the privacy of the information. There are other interesting applications such as digital signatures, the problem of authentication and the concept of digital cash to name a few. The proliferation of computer networks resulted in a large demand for cryptography from the private sector.

A basic building block in public key cryptography are the one-way trapdoor functions. These are one-one functions which can be efficiently computed. The inverse function can however only be computed if some additional trapdoor is known. The best known one-way trapdoor function is the RSA function whose difficulty of inverting is related to the difficulty of factoring. Other one-way trapdoor functions use the arithmetic of elliptic curves and more general abelian varieties,

In this talk we will first provide a survey for the non-specialists. We then explain some new ideas on how to bulid one-way trapdoor functions from actions of finite simple semi-rings on finite semi-modules. The presented results constitute joint work with Elisa Gorla, Gerard Maze and Chris Monico and Jens Zumbrägel.

Convolutional Codes and Systems over Finite Fields

Joachim Rosenthal
University of Zürich
Mathematics Institute
8057 Zürich, Switzerland

It is well known that a convolutional code is essentially a linear system defined over a finite field. Despite this well known connection convolutional codes have been studied in the past mainly by graph theoretic methods and in contrast to the situation of block codes there exist only few algebraic constructions. It is a fundamental problem in coding theory to construct convolutional codes with a designed distance.

A first part of the talk describes the connection between convolutional codes and linear systems [**?**, **?**]. Using systems theoretic methods we explain how to construct codes with maximal or near maximal free distance [**?**]. We show how decoding can be viewed as a discrete tracking problem where the received signals have to be optimally matched with a sequence generated by the encoder. We also report on recent progress in the construction of convolutional codes by algebraic means [**?**].

Convolutional codes have been used in the past mainly for the purpose of point to point communication. Recent work by Hadjicostis, Verghese, Fliess and their collaborators have shown (see e.g. [**?**]) interesting applications to Fault Tolerant systems where codes over a large alphabet play an important role. In a final part of the talk we will address these applications.

References

[1] H. Gluesing-Luerssen and W. Schmale. On cyclic convolutional codes. *Acta Appl. Math*, 82:183–237, 2004.

[2] C. N. Hadjicostis. Nonconcurrent error detection and correction in fault-tolerant linear finite-state machines. *IEEE Trans. Automat. Contr.*, AC-48(12):2133–2140, 2002.

[3] R. Hutchinson, J. Rosenthal, and R. Smarandache. Convolutional codes with maximum distance profile. *Systems & Control Letters*, 54(1):53–63, 2005.

[4] J. L. Massey and M. K. Sain. Codes, automata, and continuous systems: Explicit interconnections. *IEEE Trans. Automat. Contr.*, AC-12(6):644–650, 1967.

[5] J. Rosenthal, J. M. Schumacher, and E. V. York. On behaviors and convolutional codes. *IEEE Trans. Inform. Theory*, 42(6, part 1):1881–1891, 1996.