„Cryptology and Information Security including Knowledge Exchange and Technology Transfer"

Seminar 1: Fractal Geometry and Chaos

This seminar will provide an overview of fractal geometry used for synthesizing and analysing data coupled with the modelling of non-linear systems and chaos.

Seminar 2: Encryption Using Chaos

The seminar explains how chaotic systems can be used to design multi-algorithmic ciphers and discusses the commercialisation of this approach leading to the development of *Crypstic*^{TM} by Lexicon Data Limited.

Seminar 3: Covert Encryption Methods

One of the principal weaknesses of all encryption systems is that the *ciphertext* 'flags' the fact that the encrypted information is of value. This seminar looks at methods of 'information hiding' and data camouflage using fractal geometry and Steganography. A number of applications are considered including e-Fraud prevention and data authentication in general.

Seminar 4: Print Security and Anti-counterfeiting Methods

This seminar examines the application of print security features and technologies that are used to authenticate hardcopy documents. It introduces a new method focused on the use of low resolution print/scan devices based on *Texture Coding* and considers the range of applications to which this method of anti-counterfeiting can be applied.

Knowledge Exchange and Technology Transfer

The seminars will include aspects of research being undertaken at DIT in the Information and Communications Security Research Group which is based in DIT's Faculty of Engineering, School of Electrical Engineering Systems and

School of Electronic and Communications Engineering. The research group is headed by SFI Stokes Professor J M Blackledge who has over ten years industry experience in this area including work undertaken for the Bank of England, GCHQ, Giesecke & Devrient GmbH and Microsharp Corporation where he was formerly Director of R & D.

Along with applied and academic research, the Group also engages in consultancy and industry collaboration and has a range of proprietary technologies available for license. Research interests and expertise include the following:

- data encryption using novel algorithms
- information hiding and Steganography
- data authentication
- printed document authentication using texture coding
- forensically inert software engineering
- covert encryption methods
- management of encrypted information
- software solutions for security applications
- network security
- digital rights management

Together with a set of recent publication, details of the research being undertaken will be provided in order to exchange knowledge and to provide a transfer of technology within the context of the seminars described above. By way of an example, the Group is currently engaged in developing a major FP7 proposal – CryptoMed - for the EU commission on developing anti-counterfeiting measures to tackle the counterfeiting of drugs using a combination of print security features, including active holograms, Raman spectroscopy and Internet track and track techniques. The consortium includes the Network Security Group, Faculty of Electronics and Information Technology, Institute of Telecommunications at WUT who will be undertaking much of the Internet resources required to implement these technologies.