University of Western Sydney
Bringing knowledge to life

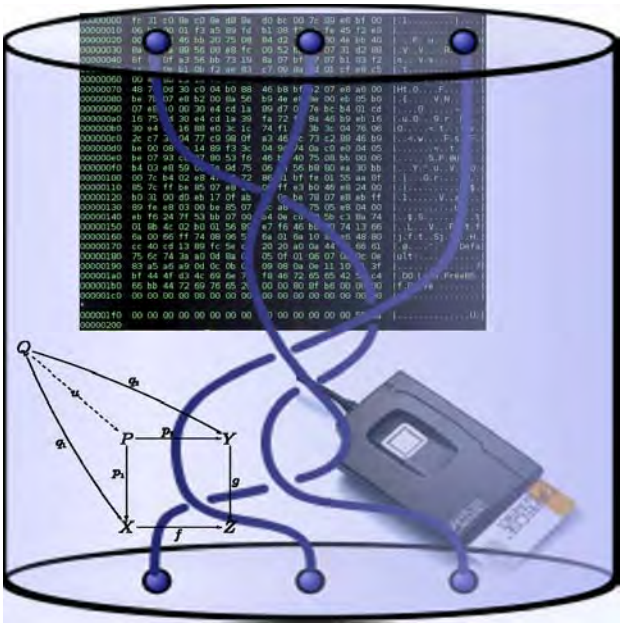
RESEARCH DIRECTIONS

Braid Theory Ties Up Data Security

Dr Volker Gebhardt from the School of Computing and Mathematics is collaborating with Professor Patrick Dehornoy from the University of Caen and Dr Juan González-Meneses from the University of Seville to explore mathematical theories that can improve data security. This project has been funded by the Australian Research Council through its Discovery Project scheme.

‘Modern life depends on the security of electronic information such as banking transactions and the accurate identification of legitimate users’, says Dr Gebhardt. ‘Many modern schemes used to protect data or to authenticate users are based on number theory, a branch of pure mathematics. Recently, another branch of pure mathematics, the theory of braid groups, has attracted interest for the purposes of data security, since it promises to achieve the same level of security with less complex and faster systems. Our project will explore the properties of braids and related mathematical objects, whose structure is as yet not fully understood. This is basic research which is interesting in its own right, but it also has ramifications for data encryption and the security of confidential personal information.’

The team has expertise in pure mathematics (group theory and combinatorics), computational algebra, and computer programming. ‘The lack of good intuition is a huge limitation for this field, one that we want to address using our strengths’, says Dr Gebhardt. Traditional theoretical mathematical investigations will be coupled with systematic and large scale computer experiments to both develop and test conjectures. Since there are no software packages to support this work, the efficient implementation of both existing and newly developed algorithms will be a necessary part of this process.



This project will strengthen Australia’s position as a centre for research in computational algebra, an area which forms the mathematical basis for new and more efficient technologies for information security and secure identification. The results can lead to new technologies for protecting confidential data, which are more efficient and hence cheaper to implement than existing alternatives. Secure identification of legitimate users in the context of online banking is one possible field of application.

Project Title: Algorithmic Approaches to Braids and their Generalisations.
Funding has been set at: $150,000
Contact Details: v.gebhardt@uws.edu.au
http://www.uws.edu.au/computing_mathematics
October 2010