“VSH: A Practical and Provable Collision Resistant Hash Function”
SPEAKER: Dr Scott Contini, Macquarie University, Australia

Abstract:
Due to the recent work of Chinese researchers lead by Xiaoyun Wang, the most widely used hash functions are known to be insecure (MD4, MD5, SHA-0) or are on the brink of being broken (SHA-1). What did we do wrong? In this talk, we start by looking at the gap between the theory and the practice of cryptographic hashing. Historically, we see that due to the lack of a practical design that agreed with the theory, the research community has taken a heuristic approach to hashing. Furthermore, there have been attempts to build a theory justifying the heuristic approach (such as random oracles), but these attempts have several shortcomings. This introduction will motivate our new design, VSH, which is a practical solution to what theoreticians have asked for from as early as 1987. VSH can be combined with Cramer-Shoup signatures to provide an entirely provable and practical real-world solution.

About the speaker:
Scott Contini received his PhD from Technische universiteit Eindhoven. He is currently a research fellow at the Centre for Advanced Computing - Algorithms and Cryptography, Macquarie University. Prior to joining in Macquarie, he spent several years at the industrial research labs including Bellcore, RSA and Motolora, and one and half years with Sydney University to develop the Magma Computer Algebra Package. Dr Contini has publications in number theory, public and private key cryptography, and hash functions.

Date : Wednesday, 14 February 2007
Time : 2.30pm to 3.30pm
Venue : MME Journal Room (NIE7-03-16)
        (NIE, Block 7, Level 3, Room 16)

ALL ARE WELCOME! (FREE ADMISSION)