THE UNIVERSITY OF MELBOURNE

MELBOURNE SCHOOL OF ENGINEERING

PhD Program offered to
IIT Kanpur, Madras and IISc students
by the Melbourne School of Engineering

Provably Secure Cryptographic Access Control

Supervisors: Dr. Udaya Parampalli

Dual PhD option: Melbourne only degree (with a stay at the overseas lab for few months)

Project description: Most of the current security applications are based on directory based crypto services and use public key infrastructure. These systems make use of random looking key materials for entities and relating the key material to the actual identity of the entities is an important authentication problem. Non directory based framework can be defined using the actual identities as the key material and this framework can handle the authentication problems in a simplified and scaled manner. This project intends to develop novel provably secure access control mechanisms using generalizations and Identity and Attribute based cryptographic schemes.

Student performance requirement: GPA of 8.5/10 or better.

Please note: the applicant must discuss with the nominated supervisor before finalizing the project proposal to be submitted to the University of Melbourne. This proposal is dedicated to IIT Kanpur, IIT Madras and I.I.Sc educated students only. The scholarship covers tuition and living expenses to work on the project. Applicants are not required to do any teaching. Duration of the PhD is 3-3.5 years and applicants can be admitted to the PhD candidature after the completion of a Masters degree or 4 year Bachelors degree from IIT Kanpur.

Rankings: The Melbourne School of Engineering is Australia's No. 1 engineering and technology school and No. 25 in the world *

Website: www.eng.unimelb.edu.au

* **Times Higher Education World University Rankings 2012-2013.**