• Z'ABA, Muhammad Reza
  BSc (Computer) University of Technology Malaysia
  Thesis Title:
  Analysis of Linear Relationships in Block Ciphers.
  Supervisors:
  Prof. Ed Dawson (Principal)
  Dr. Leonie Simpson (Associate)
  Dr. Kenneth Wong (Associate)
  Dr. Matt Henricksen (Associate)
  Dr. Håvard Raddum (Associate)
  Citation:
  This thesis presents new results on the analysis of linear relationships in block ciphers. New
  properties that have the potential to be exploited in attacks are identified. These results are
  significant because block ciphers are currently widely used as a crucial component in
  providing secrecy of messages. In this thesis, several linear relationships in block ciphers
  have been identified and used to improve existing attacks, to identify unexpected properties
  in nonlinear components, and as basis for a new measure of diffusion.

  Approved  E. Dawson