

GORANTLA, Malakondayya Choudary

B.Tech. Andhra University, M.Tech. University of Hyderabad

Thesis Title:

Design and Analysis of Group Key Exchange Protocols

Supervisors:

Dr. Juan González Nieto (Principal)

Prof. Colin Boyd (Associate)

Citation:

This thesis studies one of the most important problems in cryptography, known as group key exchange, which is vital in establishing secure group communication. It designs and analyses various group key exchange protocols which will have potential applications in satellite television, Internet video broadcasting, collaborative systems and video/audio conferencing. The security of the group key exchange protocols proposed in this thesis have been analysed with mathematical rigour using the computational complexity approach.