ORAL DEFENSE ANNOUNCEMENT

Nguyen Phuong Ha

ON DESIGN AND ANALYSIS OF SYMMETRIC KEY CIPHERS

Abstract:

This thesis studies the cryptanalysis and design of some cryptographic algorithms in symmetric key ciphers. Block ciphers and Stream ciphers are two backbone elements in symmetric key ciphers. We cryptanalyze ZUC stream cipher, SERPENT, KASUMI and SMS4 block ciphers by using some new improved cryptographic methodologies, tools and algorithms. Based on the results obtained in cryptanalysis, we propose some modifications in the designs of ZUC, KASUMI and SMS4 to enhance their security. Additionally, we introduce several methodologies to enable and efficiently implement 3-share Threshold Implementation to any 4-bit S-box. Threshold Implementation is widely accepted as a countermeasure against first order Differential Power Analysis in Side Channel Attack and 3-share version is the most efficient in terms of hardware implementation. To support the theoretical results, we construct 3-share Threshold Implementations to S-boxes of PRESENT, SERPENT ciphers. Notably, 3-share version was believed to be not possible for some S-boxes of SERPENT until now.

Date: 22 January 2013 (Tuesday)
Time: 10.00am
Venue: NTU SPMS MAS Building Level 3
        MAS Executive Classroom 1, MAS-03-06
Supervisor: Assoc Professor Wang Huaxiong