MSc Thesis Pre-Proposal

Optimizing Confusion and Diffusion in Symmetric-Key Cryptographic Algorithms

Christopher A. Wood
Department of Computer Science
Rochester Institute of Technology
caw4567@rit.edu

May 13, 2012

Abstract

The thesis proposal is a type of contract between the faculty and the student. An accepted thesis proposal indicates that the work proposed by the student, once completed, will be accepted by the faculty as sufficiently innovative and substantial as to be recognized with the award of the degree. It is part of the training of the student's research apprenticeship that the form of this proposal must be as concise as those proposals required by major funding agencies.

Contents

1 Introduction

This part provides an overall introduction of your work, including related work of your proposal.

1.1 Related work

This part talks about related work of your proposal.

2 Cryptanalysis Attack Review

TODO: linear, differential,

3 Mathematical Analysis of Existing Cryptographic Operations

The content of your proposal. Each topic occupies one section, each with their own conclusion and future work.

3.1 Confusion through Nonlinear Operations

TODO: S-boxes, ARX, Chaos, etc

4 Diffusion and Confusion MINLP Problems

TODO: formulate algorithm security as MINLP problems, explore usage of evolutionary algorithms to perform intelligent search over design space

5 Implementation Considerations of Cryptographic Operations

The content of your proposal. Each topic occupies one section, each with their own conclusion and future work.

5.1 Software Implementations

TODO

5.2 Hardware Designs

TODO

6 Research Methodology

TODO

7 Potential Outcomes

TODO