4040-849 Optimization Methods

Written Assignment 1

Christopher Wood

March 27, 2012

Abstract

Optimization of number of rounds in cryptographic primitive (block cipher like AES) versus time to compute. Need to maximize the diffusion and confusion from the cipher.

TODO: maximize randomness output (combination of confusion and diffusion) TODO: figure out a randomness equation for costs TODO: define design variables - the number of rounds

constraints: number of rounds is limited constraints: execution time is limited