

Cube Attacks on Cryptographic Hash Functions

Master's Thesis Defense Announcement

Joel Lathrop
Department of Computer Science
Rochester Institute of Technology
jal6806@cs.rit.edu

Chair:	Stanisław Radziszowski	spr@cs.rit.edu
Reader:	Christopher Homan	cmh@cs.rit.edu
Observer:	Edith Hemaspaandra	eh@cs.rit.edu

Defense Date: Thursday, 5/21/09 at 11 A.M.
Defense Location: 70-1620

Abstract

Cryptographic hash functions are a vital part of our current computer systems. They are a core component of digital signatures, message authentication codes, file checksums, and many other protocols and security schemes. Recent attacks against well established hash functions have led NIST to start an international competition to develop a new hashing standard to be named SHA-3.

In this thesis, we provide cryptanalysis of some of the SHA-3 candidates. We do this using a new cryptanalytical technique introduced a few months ago called Cube Attacks. In addition to summarizing the technique, we build on it by providing a framework for estimating its potential effectiveness for cases too computationally expensive to test. We then successfully apply cube attacks to reduced round variants of the ESSENCE and Keccak SHA-3 candidates and provide a detailed analysis of how and why the cube attacks succeeded as well as limits for their extension into theoretical attacks on higher round variants of these hashes. Finally, we provide some preliminary results of applying cube attacks to other SHA-3 candidates.