Rotacrypt: Rotational Mechanics as a Cryptographic Primitive

Teo Honda Scully

Abstract

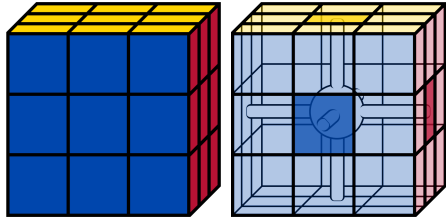...TBD...

Contents

1 Introduction

¡···¿

1.1 Review of Rubik's Cubes

1.2 Scheme Overview

¡···¿

1.3 Intended Usage

¡···¿

2 3x3x3 Implementation

¡···¿

2.1 Data Structure Breakdown

¡···¿

2.2 Augmented SPEFFZ Mapping

¡···¿

2.3 Cyclic Transformations

3 Key Generation

¡···¿

3.1 4-Cube Initialization

¡···¿

3.2   Master-Key Serialization

ï…¿

3.3   Sub-Key Generation

ï…¿

4   Encryption

ï…¿

4.1   Plaintext Setup With S-Box Transformations On Chunks

ï…¿

4.2   Cube Mapping Procedure

ï…¿

4.3   Encryption Algorithm

ï…¿

5   Decryption

ï…¿