

Rotacrypt: Rotational Mechanics as a Cryptographic Primitive

Teo Honda Scully

Abstract

...TBD...

Contents

1	Introduction	2
1.1	Review of Rubik's Cubes	2
1.2	Scheme Overview	2
1.3	Intended Usage	2
2	3x3x3 Implementation	2
2.1	Data Structure Breakdown	2
2.2	Augmented SPEFFZ Mapping	2
2.3	Cyclic Transformations	2
3	Key Generation	2
3.1	4-Cube Initialization	2
3.2	Master-Key Serialization	2
3.3	Sub-Key Generation	2
4	Encryption	3
4.1	Plaintext Setup With S-Box Transformations On Chunks	3
4.2	Cube Mapping Procedure	3
4.3	Encryption Algorithm	3
5	Decryption	3

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

...

3.3 Sub-Key Generation

...

4 Encryption

1...6

4.1 Plaintext Setup With S-Box Transformations On Chunks

1...6

4.2 Cube Mapping Procedure

1...6

4.3 Encryption Algorithm

1...6

5 Decryption

1...6