Rotacrypt: Rotational Mechanics as a Cryptographic Primitive

Teo Honda Scully

Abstract

...TBD...

Contents

1 Introduction

¡···¿

1.1 Review of Rubik's Cubes

Ah, the Rubik's Cube—the iconic toy that bedevils and delights in equal measure. Born from the ingenious mind of Ernő Rubik in 1974, it's more than just a puzzle. Forget mere child's play; this cube is chaos in the physical. Just kidding. To go from the state of chaos to order, one only needs to know a solving protocol of which many exist.

Max Park, the current world record holder (11 June 2023) for the 2-handed solve, obliterated the cube in a mind-blowing 3.13 seconds. Lucky scramble? Hardly. Yiheng Wang, who holds the world record average-of-five, clocks in at a dizzying 4.48 second mean solve time throughout the five solves.[1] And no, I won't depress you by mentioning his tender age of nine years old. But let's not divert. The Rubik's Cube–a mathematical marvel and a cipher waiting to be cracked.

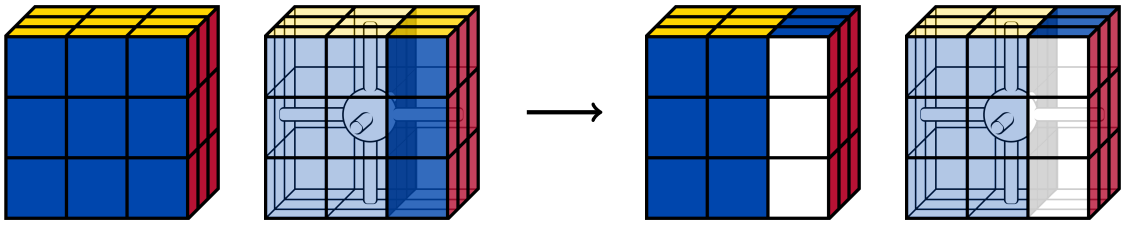
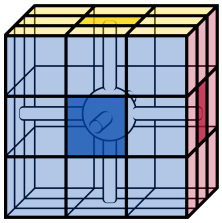


Figure 1: A visualization of the R operation (rotating the right layer clockwise).

Let's dive into the details of the mechanics of the 3x3x3 puzzle. The cube boasts centers, edges, and corners. These center pieces serve as the invariant axis around which the peripheral cubies rotate. The six unit colors are yellow, blue, red, green, orange, and white.



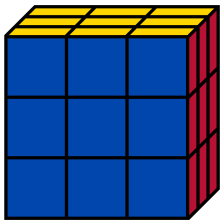
A visualization of a 3x3x3 cube. The cube has 6 faces, each with 9 stickers. Notably, this means that there exists 54 different unit tiles on the cube. The cube has 43,252,003,274,489,856,000 possible states.[2]

For instance, if the cube is held with a yellow top and blue front, the red and orange faces will invariably be to the right and left, respectively. In fact, the red and orange center pieces will *always* be opposites, as will the blue-green and white-yellow pairs of center pieces.

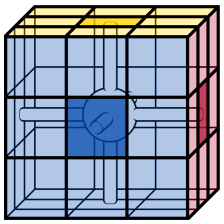
[1] An average-of-five is determined by taking the average of the three "middle" solves in a session of five scramble. In other words, the worst and best solve time are dropped from the calculation for the average.

[2] This number is calculated by considering the 8 corners, each with 3 orientations, and the 12 edges, each with 2 orientations.

With fixed center pieces, this means that a static orientation, such as holding the cube with the yellow face on the top layer and the blue face on the front layer (as pictured above) yields an orientation in which the red face will always be to the right, the green face always to the left,



A visualization of a 3x3x3 cube. The cube has 6 faces, each with 9 stickers. Notably, this means that there exists 54 different unit tiles on the cube. The cube has 43,252,003,274,489,856,000 possible states.



The six colors of the cube are Yellow, Blue, Red, Green, Orange, and White. The cube has 6 center pieces, and they are permanently fixed in place. The center pieces are the only pieces that have a single color, and they do not move when the cube is being solved.

The center pieces are permanently affixed to the core. These center pieces serve as the invariant axis around which the peripheral cubies rotate.

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

¡...¿

4.1 Plaintext Setup With S-Box Transformations On Chunks

¡...¿

4.2 Cube Mapping Procedure

¡...¿

4.3 Encryption Algorithm

¡...¿

5 Decryption

¡...¿