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.

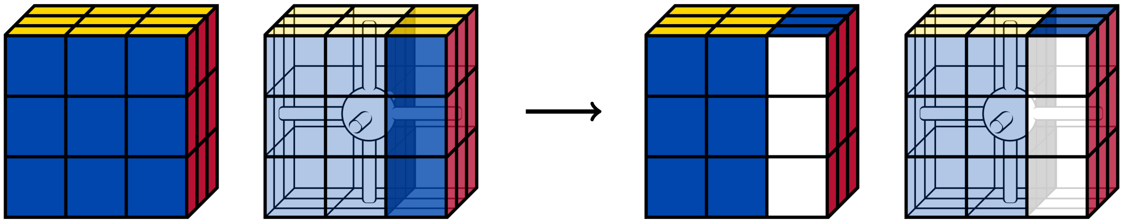
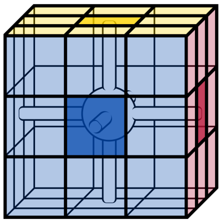


Figure 1: A visualization of the R operation (rotating the right layer clockwise).

Let’s dive into the mechanics of the 3x3x3 puzzle. The cube boasts centers, edges, and corners. These single-colored 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.

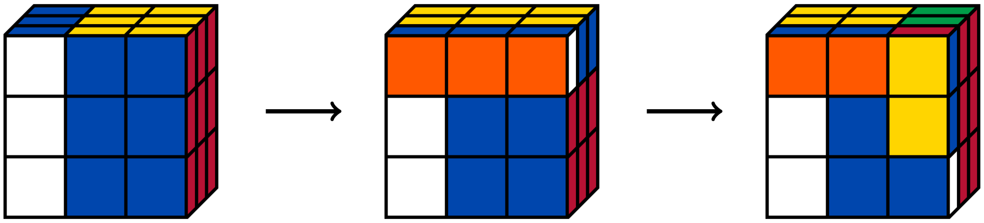


Figure 2: A visualization of the *L' U' R'* operation(s).

1.2 Notation for Cube Operations

The notation used to describe the movements and algorithms for solving the Rubik's Cube is standardized to facilitate easy understanding and sharing of solutions. Each face of the cube is designated by an uppercase letter:

- **U** - Up (Top Layer)
- **D** - Down (Bottom Layer)
- **L** - Left (Left Layer)
- **R** - Right (Right Layer)
- **F** - Front (Front Layer)
- **B** - Back (Back Layer)

The following symbols are appended to these letters to indicate the direction of rotation:

- No symbol - 90-degree clockwise rotation
- **'** (apostrophe) - 90-degree counterclockwise rotation
- **2** - 180-degree rotation (either direction)

For example, the sequence *L' U' R'* would indicate a counterclockwise rotation of the left layer, followed by a counterclockwise rotation of the top layer, and finally, a counterclockwise rotation of the right layer.

1.3 God's Number

In the realm of 3x3x3 Rubik's Cubes, *God's Number* is a term used to denote the maximum number of moves required to solve any scrambled cube. It has been proven that any cube can be solved in 20 moves or fewer (the citation can be found in the *References* section). This concept is an intriguing insight into the mathematical efficiency of the cube's design.

Furthermore, this means that any scramble can be reached with 20 moves or fewer. This is a key point to keep in mind when considering the security of the cube as a cryptographic primitive as well as for key size considerations.

1.4 Combinatorial Explosion with Multiple Cubes

Let us consider the number of possible states for a single 3x3x3 Rubik's Cube, which is $43,252,003,274,489,856,000$. When chaining together the combinations of two different cubes, the number of combined states is $(43,252,003,274,489,856,000)^2$.

This squaring occurs because each state of the first cube can pair with every state of the second cube, yielding $43,252,003,274,489,856,000 \times 43,252,003,274,489,856,000$. Mathematically, the set of possible states becomes the Cartesian product of the two sets of states, leading to an exponential increase in complexity.

One intriguing aspect of chaining multiple Rubik's Cubes is the exponential growth in the state space. Let N represent the number of unique states for a single Rubik's Cube. For k chained Rubik's Cubes, the total number of unique states becomes N^k. This exponential increase serves a critical function: it substantially minimizes the likelihood of collisions whilst simultaneously increasing the difficulty of brute-force attacks.

2 Overview

2.1 Scheme Overview

¡…¿

2.2 Purpose

There is no purpose. I was told to not make a cryptosystem, so I did the opposite.

2.3 Intended Usage

¡…¿

3 3x3x3 Implementation

¡…¿

3.1 Data Structure Breakdown

¡…¿

3.2 Augmented SPEFFZ Mapping

¡…¿

3.3 Cyclic Transformations

4 Key Generation

¡…¿

4.1 4-Cube Initialization

¡…¿

4.2 Master-Key Serialization

¡…¿

4.3 Sub-Key Generation

¡…¿

5 Encryption

¡…¿

5.1 Plaintext Setup With S-Box Transformations On Chunks

¡…¿

5.2 Cube Mapping Procedure

¡…¿

5.3 Encryption Algorithm

¡…¿

6 Decryption

¡…¿