Nash Stream Cipher: A Hardware-Optimized Implementation

[Author]

December 22, 2024

Abstract

This document presents a modern hardware implementation of John Nash's stream cipher, originally proposed to the NSA in 1955. The implementation features auto-synchronization capabilities, error recovery, and resistance to side-channel attacks.

1 Algorithm Specification

1.1 State Machine

The cipher consists of two permutation paths (red and blue) through a state machine with the following properties:

- State transitions defined by permutation functions
- Bit inversion operations (+/-) at specific states
- Auto-synchronization through feedback mechanism

2 Security Analysis

2.1 Computational Security

Nash's exponential conjecture states that for sufficiently complex enciphering systems, the computational work required to break them grows exponentially with key length...

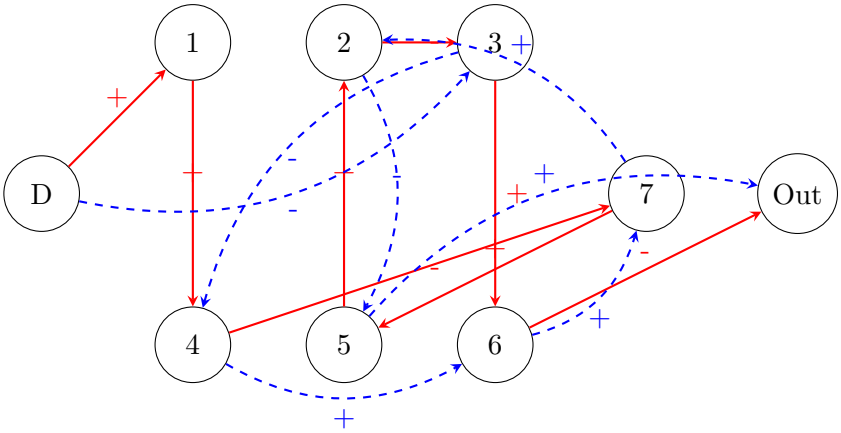

Figure 1: Nash Cipher State Machine Diagram

3 Hardware Implementation

3.1 Resource Requirements

- State machine logic
- Memory elements
- Permutation path routing