CALIFORNIA STATE SCIENCE FAIR
2010 PROJECT SUMMARY

Name(s) **Akshay Nathan**	**Project Number** **S1612**

Project Title

A Super-Encryption Standard for Large Data Using Elementary Chaotic Cellular Automata

Abstract

Objectives/Goals

Cellular Automata are arrays of bits that evolve according to a rule. Some automata exhibit chaotic and random behavior which indicates that they have potential for encryption. Many other attempts at building an encryption system have been vulnerable to certain types of attacks. The goal of this project was to create and implement a novel encryption scheme based on cellular automata, and to evaluate its randomness, efficiency, and strength.

Methods/Materials

Each preliminary algorithm was implemented in C and tested using government recommended statistical tests. The final algorithm passed all of the tests multiple times, and exhibited better randomness qualities than some supposedly "true" random number generators. The algorithm was also timed, and growth analysis showed that with optimization, the scheme would be as fast as or faster than industry standard stream ciphers such as RC4.

Results

The final algorithm takes an input of a 3-part key and a plaintext. A unique aspect of this scheme is that the plaintext itself is run through a CA and decrypted through a designed inverting algorithm. The final ciphertext can only be broken knowing all 3 parts of the key.

Conclusions/Discussion

By using super encryption through a repeated sub-algorithm and by using a larger key, the scheme bypassed many of the attacks that are used against stream ciphers today. Although they display very complex behavior, cellular automata operations are very simple, and can be easily integrated into hardware. Additionally, this stream cipher is extremely conducive to parallel processing, making it ready for future computers. The results of this project demonstrate the practicality of cellular automata based stream ciphers by presenting a simple but elegant prototype that is secure and efficient.

Summary Statement

I created an encryption scheme using chaotic and random systems called cellular automata.

Help Received