CALIFORNIA STATE SCIENCE FAIR
2006 PROJECT SUMMARY

Name(s)

George Chen; Frank Fu-Han Chuang; Victor Andrew Shia

Project Number

S1202

Project Title

Paladin: A New Fast and Secure Symmetric Block Cipher

Abstract

Objectives/Goals

The advanced encryption standard, AES, is the standard for encryption in the United States. However, AES carries with it some flaws that may jeopardize its security. This project serves the purpose of developing a new cipher that addresses these issues while inheriting the good aspects of many cipher designs.

Methods/Materials

Utilizing and improving upon past research and existing cipher designs, various functions of a cipher were coded to maximize security and efficiency. After compiling all of the functions into the overall cipher, several programs were coded to compare the encryption and decryption speeds of AES and Paladin and to test Paladin's resistance to certain attacks.

Results

On the Athlon, Sempron, Athlon 64, and Pentium 4 processors, Paladin encrypts and decrypts at a faster speed than several optimized software implementations of the full 14-round AES. Differential cryptanalysis and linear cryptanalysis both have complexities that make them less feasible than an exhaustive key search. Several other attacks are prevented due to Paladin's design.

Conclusions/Discussion

Paladin is faster than AES on modern systems while addressing security issues brought up with AES and various other ciphers. However, further work needs to be done in the area of cryptanalysis before Paladin can be used in a commercial environment.

Summary Statement

Paladin is a computer encryption program that protects sensitive data from unauthorized users.

Help Received

none