CALIFORNIA STATE SCIENCE FAIR
2004 PROJECT SUMMARY

Name(s)
Emily F. Eder

Project Number
S1205

Project Title
The Effect of Quantum Computing on Hash Functions

Abstract

Objectives/Goals
The purpose of this research project is to determine the effect quantum computing will have on current message authentication techniques. Attack algorithms using classical computers cannot defeat authentication methods because of space and time limitations. An efficient quantum hash function attack, based on the birthday attack, will be developed, dramatically reducing both space and time requirements for this birthday attack algorithm. This work will show that current message authentication methods must be significantly modified to defend against quantum attacks.

Methods/Materials
First, known quantum computing algorithms and hash function attack methods are analyzed. Hash values for multiple inputs are also tested, using the Sha-1 and MD5 hash algorithms. A detailed analysis of the birthday attack is performed, detecting weaknesses and postulating solutions to those weaknesses. The birthday attack then becomes the target algorithm for the remainder of the project. Next, appropriate quantum algorithms are explored in detail, and ideas that could transfer to the birthday attack are found. A quantum simulator is obtained, and known quantum algorithms are tested. Quantum algorithms are also adapted to produce different outputs. Finally, a new and original quantum birthday attack algorithm is proposed.

Results
An efficient quantum birthday attack algorithm has been created. The space requirement for this algorithm is 4n bits, where n is the size of the hash function output. The time requirements for the algorithm have also been greatly reduced. In addition, aspects of the algorithm have been simulated using a quantum simulator.

Conclusions/Discussion
The quantum birthday attack algorithm, developed in this project, gives dramatic improvements compared to the original classical algorithm. It provides a change in the space complexity from an exponential function, O(^(2n/2)), using a classical computer, to a polynomial function, O(n), using a quantum computer. This algorithm will have major implications for current message authentication procedures once quantum computing becomes a reality. Internet commerce, banking, and communication depend critically on having secure message/monetary transfers. This research has shown that message authentication techniques used for these procedures will need to be dramatically altered.

Summary Statement
An efficient quantum birthday attack algorithm has been created, which dramatically reduces space and time requirements, making current message authentication procedures vulnerable.

Help Received
Dr. V. E. Henson, Dr. E. Chow, and Mr. T. Brugger, all of LLNL, provided encouragement on my quantum research. Dr. Henson provided a linux-based laptop for quantum simulations. Prof. D. Meyer, UCSD, gave instruction on the Grover Search Algorithm.