

Title: “Identity Based Encryption in a System to Prevent Phishing Attacks”
Student: Chris Baker
Advisor: Dr. M. Atallah

With internet and computer fraud on the rise, steps need to be taken to proactively protect the average user. “Phishing” attacks are a particularly effective type of internet fraud. In these attacks, the attacker sets up a fake copy of a legitimate website in order to trick users into entering personal information. The attacker then sends out thousands of e-mails that appear to come from the legitimate site but direct users to the fake site. It is suspected that, on average, 5% of users who receive the e-mail are tricked into entering private information. Because these attacks are so effective, the number of attacks is increasing at about 26% per month.

The goal of this project is to examine the feasibility of using Identity Based Encryption to prevent Phishers from recovering a user’s private data. Identity Based Encryption is a public key crypto system in which the public key can be any arbitrary string, and the private key can be calculated by a central key generator that knows certain private parameters for the system.