6.857 Term Paper Proposal
Differential Fault Analysis

Jered Floyd (*jered@mit.edu*)
Kevin Fu (*fubob@mit.edu*)
Peter Sun (*petersun@mit.edu*)

November 5, 1996

Differential fault analysis (DFA), although not an entirely new subject, has recently been highlighted by three simultaneous publications concerning storage of cryptographic keys on *tamper-proof devices*: Bellcore's public-key attack; Biham and Shamir's attack on DES and generic secret-key algorithms; and a National University of Singapore group's attacked on RSA. The attacks are not of the algorithms themselves, but of specific implementations on tamper-proof devices.

We will create a software simulation of DFA on an abstract tamper-proof device which contains keys for a cryptosystem. Prospective algorithms include DES, RC5, and RC4.

The goal of our project is to show that under a general software abstraction of tamper-proof devices containing cryptographic keys, that the keys can be extracted by DFA with minimal effort.

We will furthermore compare and analyze different threat models to demonstrate the importance of fault tolerance in tamper-proof cryptographic hardware devices.