FPGA RFID Utility

6.111 Final Project Abstract
Hannah Field, Miles Dai

Radio Frequency Identification (RFID) forms the cornerstone of MIT's access control system. Embedded within each student's ID card is an IC and solenoid, which receives power from the 125kHz sine wave transmitted by MIT card readers. In response, the solenoid transmits the IC's bits on a 62.5kHz and 187.5kHz signal. In this project, we aim to build an RFID reader and spoofer. Using the FPGA, we will read the the signal broadcast by the card, decode it into bits, and store the bits for later replay. As the second part of the project, we will turn the FPGA into an arbitrary signal generator to turn the stored bits into a phase-shift-keyed sine wave, spoofing the signal sent by the ID card. We have two stretch goals for our project. First, we would like to make our system compatible with 13.56 MHz RFID cards. Second, we would like to investigate the process of magnetically programming bits onto blank RFID cards, thus allowing us to produce duplicate cards.