

Requirements

Team: The Locksmiths: Aaron Loomis, Joseph Medina, Vicky Lym, Erin Gurnett, Jaziel Pauda

Project: Resource Locking - 4-Bit/2-Disclosure Devices

Date: 09/08/2017

Functional

1.1 Upon Device creation

1.1.1 The number of bits must be specified.

1.1.2 Each bit must have a value of T or F.

1.2 Device capabilities

1.2.1 Must have a way to rotate the bits a random number of times in a spin operation.

1.2.2 The device must allow only limited observation of its state.

1.2.3 The device must allow only limited modification of its state.

1.2.4 The device must allow modification of bits following a peek operation.

1.2.5 A spin operation must follow either a peek, poke, or spin operation.

1.2.6 A spin operation must allow for shifting all bits one position to the circular right, an unspecified number of times.

1.2.7 A peek operation must follow a spin operation.

1.2.8 A poke operation must follow a peek operation.

1.2.9 Poke must be the only operation that allows a change to the state of any bit.

1.3 Unlocker capabilities

1.3.1 It must set all the bits to the same value.

1.3.2 The unlocker process must halt at some point, whether true or false is returned.

1.3.3 Usage of the peek() command must use a bit pattern where at least two of the bits have a ? and the other two have a -.

Non-Functional

2.1 Device Unlocker can unlock a device in a reasonable amount of time.